การพัฒนาศูนย์คอมพิวเตอร์ให้ตรงตามมาตรฐาน ISO 27001
กรณีศึกษา บริษัท ไทยลู้บเบส จำกัด (มหาชน)
DEVELOPING DATA CENTER BASED ON ISO 27001 STANDARD
CASE STUDY: THAI LUBE BASE PUBLIC COMPANY LIMITED

นางสาววรรณภา มงคลกิจจาวงศ์

โครงงานสหกิจนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีไทย – ญี่ปุ่น

พ.ศ.2554

การพัฒนาศูนย์คอมพิวเตอร์ให้ตรงตามมาตรฐาน ISO 27001

กรณีศึกษา บริษัท ไทยลู้บเบส จำกัด (มหาชน)

DEVELOPING DATA CENTER BASED ON ISO 27001 STANDARD

CASE STUDY: THAI LUBE BASE PUBLIC COMPANY LIMITED

นางสาววรรณภา มงคลกิจจาวงศ์

โครงงานสหกิจนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีไทย – ญี่ปุ่น

พ.ศ.2554

คณะกรรมการสอบ

..... ประธานกรรมการสอบ

(อาจารย์ ต่อเกียรติ ใต้ธงชัย)

..... กรรมการสอบ และอาจารย์ที่ปรึกษา

(อาจารย์ศิษฏ์ชฎา อ่ำเทศ)

..... กรรมการ

(อาจารย์ บัญชา บริคุต)

บทสรุป

ชื่อโครงงาน	การพัฒนาศูนย์คอมพิวเตอร์ให้ตรงตามมาตรฐาน ISO 27001 กรณีศึกษา บริษัท ไทยลู้บเบส จำกัด (มหาชน) พ.ศ. 2554 DEVELOPING DATA CENTER BASED ON ISO 27001 STANDARD CASE STUDY: THAI LUBE BASE PUBLIC COMPANY LIMITED 2011
ผู้เขียน	นางสาววรรณภา มงคลกิจจาวงศ์
คณะ	วิศวกรรมศาสตร์ สาขาวิชา วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ศิษฏ์ชฎา อ่ำเทศ
พนักงานที่ปรึกษา	คุณเอกพจน์ ชมภูศรี
ชื่อบริษัท	บริษัท ไทยลู้บเบส จำกัด (มหาชน)
ประเภทธุรกิจ / สินค้า	การผลิตน้ำมันหล่อลื่น

งานที่ปฏิบัติ

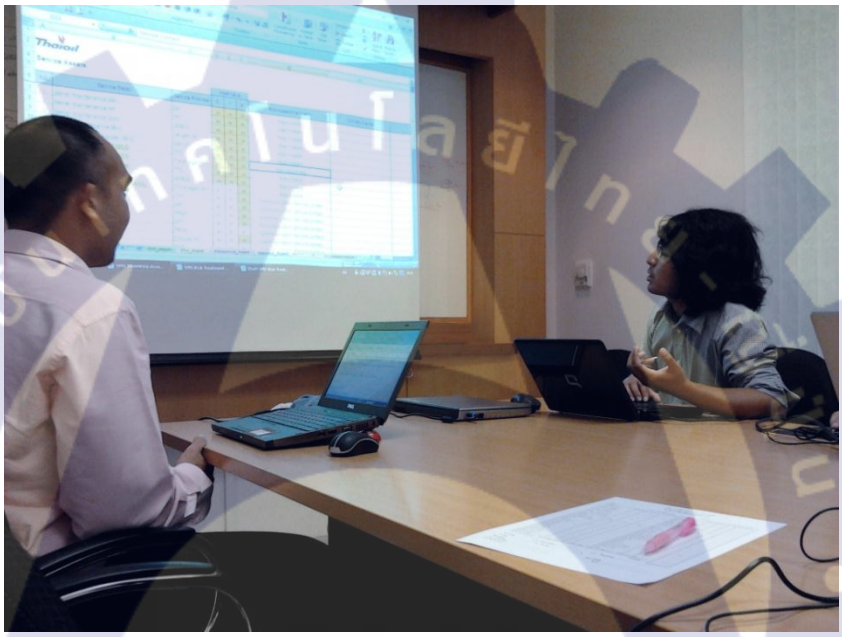
1. การทำรายการทรัพย์สินที่อยู่ในห้อง ศูนย์คอมพิวเตอร์ (Data Center)
2. การวิเคราะห์ระบบใน ศูนย์คอมพิวเตอร์ (Data Center) เพื่อป้องกันภัยคุมคามที่เกิดกับศูนย์คอมพิวเตอร์ (Data Center)
3. ออกแบบวิธีการเก็บรักษาข้อมูล เช่น เอกสาร สื่อบันทึกข้อมูล เป็นต้น
4. การปรับห้องศูนย์คอมพิวเตอร์ (Data Center) ให้ได้มาตรฐานตาม ISO 27001
5. การจัดทำนโยบายความปลอดภัยในศูนย์คอมพิวเตอร์ (Data Center)

ผลที่ได้รับจากการดำเนินงานและประโยชน์ที่ได้รับ

1. มีนโยบายที่เป็นมาตรฐานมีการลงลายลักษณ์อักษรทำให้มีความน่าเชื่อถือ
2. ทำให้ระบบสารสนเทศทำงานอย่างมีประสิทธิภาพและมีความปลอดภัยสูง
3. เนื่องจากการมีข้อมูลและระบบการจัดเก็บข้อมูลที่มีความปลอดภัย และมีประสิทธิภาพพร้อมใช้งานเสมอนั้นย่อมช่วยสร้างความได้เปรียบทางการแข่งขันสร้างผลกำไร และสร้างโอกาสทางการธุรกิจ
4. สร้างความมั่นใจให้กับลูกค้า รับประกันความต่อเนื่องในการทำธุรกิจระหว่างคู่ค้า

5. รับรู้ถึงการประเมินความเสี่ยง การแยกแยะภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้น ทำให้ทราบถึงจุดอ่อนและความเป็นไปได้ของความเสี่ยงจากการพิจารณาอย่างถี่ถ้วนของผลกระทบที่จะเกิดทำให้แก้ไขปัญหานั้น ๆ ให้มีผลกระทบต่อองค์กรน้อยลงหรือลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

รูปถ่ายผลงานสหกิจศึกษาที่ได้ดำเนินการ



กิตติกรรมประกาศ

โครงงานศึกษาค้นคว้านี้สำเร็จลุล่วงได้ด้วยความกรุณาจากคุณเอกพจน์ ชมพูศรี พนักงานที่ปรึกษา และอาจารย์ศิษฏ์ชฎา อ่ำเทศ อาจารย์ที่ปรึกษา ซึ่งท่านได้ช่วยเหลือถ่ายทอดความรู้และแนะนำแนวทางในการปฏิบัติงาน และให้คำแนะนำในเรื่องต่าง ๆ เป็นอย่างดี

อีกทั้งความช่วยเหลือ และกำลังใจความอุปการะจากครอบครัว เพื่อน ๆ และขอขอบคุณบริษัท ไทยลู้บเบส จำกัด (มหาชน) ที่ให้ความอนุเคราะห์รับข้าพเจ้าเข้ามาสหกิจศึกษากับทางบริษัท พีรสุต ศรีธวัช ณ อยุธยา และนางสุพรรณี ฟูกำเนิด ที่ให้โอกาสข้าพเจ้าเข้ามาปฏิบัติงานกับฝ่าย แผนกลยุทธ์ (SPIS) พี่พนักงานฝ่าย SPIS ทุกท่าน ที่ช่วยให้ความรู้ คำปรึกษาชี้แนะ และความช่วยเหลือเสมอมา และสุดท้ายนี้ข้าพเจ้าขอขอบคุณสถาบันเทคโนโลยีไทย-ญี่ปุ่นที่ให้โอกาสข้าพเจ้าในการศึกษาเรียนรู้ และฝึกทักษะในด้านต่าง ๆ ขอขอบคุณทุกท่านมา ณ โอกาสนี้ ด้วย

นางสาววรรณภา มงคลกิจจาวงศ์
ผู้จัดทำโครงงานสหกิจ

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญ (ต่อ)

รายการตาราง

รายการรูปประกอบ

รายการรูปประกอบ (ต่อ)

รูป **หน้า**

บทที่ 1 บทนำ

1.1 ชื่อและที่ตั้งของสถานประกอบการ

บริษัท ไทยลู้บเบส จำกัด (มหาชน)

รูปที่ 1.1 โลโก้บริษัทไทยลู้บเบส

อาคารไทยลู้บ เลขที่ 163/19 หมู่7 ต.ทุ่งสุขลา อ.ศรีราชา จ.ชลบุรี 20230

รูปที่ 1.2 แผนที่บริษัท ไทยลู้บเบส

1.2 ลักษณะธุรกิจของสถานประกอบการ หรือการให้บริการหลักขององค์กร

1.2.1 ประวัติ

ผู้ดำเนินกิจการโรงกลั่นน้ำมันหล่อลื่นพื้นฐานแห่งแรกของประเทศไทย โดยวัตถุประสงค์ในการก่อตั้งนั้นมาจาก มติของคณะรัฐมนตรี ที่ต้องการลดการพึ่งพาและการนำเข้าน้ำมันหล่อลื่นพื้นฐานจากต่างประเทศ และเพื่อเป็นการพัฒนาอุตสาหกรรมปิโตรเลียมให้ครบวงจร คณะรัฐมนตรีจึงมีมติให้การปิโตรเลียมแห่งประเทศไทย ร่วมกับ บริษัท ไทยออยล์ จำกัด บริษัท มิตซูบิชิ ออยล์ จำกัด และบริษัท บีพี ออยล์ (ประเทศไทย) จำกัด ลงนามร่วมทุนจัดตั้ง บริษัท ไทยลู้บเบส จำกัด เมื่อเดือนมีนาคม 2536 โดยก่อตั้งโรงกลั่นที่ถนนอ่าวอุดม อำเภอศรีราชา จังหวัดชลบุรี บนพื้นที่กว่า 130 ไร่

ใน วันที่ 28 มีนาคม 2539 ได้ทำการจดทะเบียนแปรสภาพเป็นบริษัทมหาชนจำกัด โดย มีชื่อใหม่ว่า บริษัท ไทยลู้บเบส จำกัด (มหาชน) และในวันที่ 28 พฤศจิกายน 2540

สมเด็จพระเทพรัตนราชสุดา สยามบรมราชกุมารี เสด็จพระราชดำเนินทรงเปิดโรงกลั่นน้ำมันหล่อลื่นพื้นฐานศรีราชา และเริ่มดำเนินการผลิตน้ำมันหล่อลื่นพื้นฐานในเชิงพาณิชย์ นับตั้งแต่ วันที่ 1 มกราคม 2541 เป็นต้นมาถึงปัจจุบัน

1.2.2 ผลิตภัณฑ์

ผลิตน้ำมันหล่อลื่นพื้นคุณภาพสูง ซึ่งประกอบด้วยน้ำมัน Solvent Neutral Oil (SNO) และ Bright Stock รวม 4 ชนิด ผลิตภัณฑ์หลัก ได้แก่

1) 60 SN เป็นวัตถุดิบในการผลิตน้ำมันหล่อลื่นประเภทส่งกำลัง น้ำมันหม้อแปลงไฟฟ้าใช้กับเครื่องทำความเย็น

2) 150 SN เป็นวัตถุดิบเพื่อผลิตเป็นน้ำมันหล่อลื่นที่ใช้ในอุตสาหกรรมการผลิตทุกชนิด เช่น อุตสาหกรรมรถยนต์ อุตสาหกรรมขนส่ง

3) 500 SN เป็นวัตถุดิบในอุตสาหกรรมการผลิตน้ำมันหล่อลื่นสำหรับรถยนต์เกือบทุกประเภท เช่น รถยนต์ส่วนบุคคล รถบรรทุก รถจักรยานยนต์ เป็นต้น

4) 150 BS สามารถ นำไปใช้ในอุตสาหกรรมและเครื่องจักรที่มีแรงเสียดทานมาก เช่น ใช้ในเครื่องยนต์ของบรรทุก เครื่องจักรรถไฟ เครื่องยนต์เรือเดินทะเล และอุตสาหกรรมยางสังเคราะห์

1.2.3 ผลิตภัณฑ์พิเศษ

TDAE สารสกัดอะโรเมติกที่ผ่านการบำบัดแล้ว (Treadted Distillate Aromatics Extract) หรือเรียกอีกชื่อหนึ่งว่า น้ำมันยางมลพิษต่ำ (Lox-Toxic Rubber Processing Oil) Wax วัตถุดิบในการผลิตเทียนไข เครื่องสำอางค์ และภาชนะบรรจุหีบห่อ

1.2.4 ผลิตภัณฑ์พลอยได้

Extract สารอะโรเมติกเป็นวัตถุดิบในการผลิตยางและยางสังเคราะห์เกือบทุกชนิด เช่น ยางรถยนต์ พื้นรองเท้า โดยสามารถผลิตได้ 4 ชนิดคือ

1) 60 Extract
2) 150 Extract
3) 500 Extract
4) BS Extract

กำมะถัน เป็นวัตถุดิบในการผลิตผงซักฟอกและแบตเตอรี่รถยนต์

แนฟทา เป็นวัตถุดิบในการผลิตน้ำมันเบนซิน

Bitumen เป็นวัตถุดิบจากการกลั่นน้ำมัน

1.2.5 กระบวนการผลิต

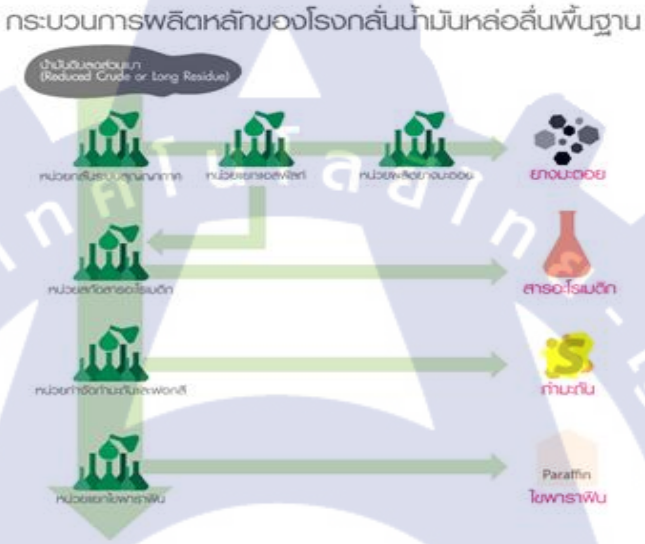
หน่วยกลั่นสุญญากาศ (Vacuum Distillation Unit) เป็นหน่วยแรกของระบบการผลิต มีหน้าที่ในการกลั่นแยกชนิดของน้ำมันตามลำดับอุณหภูมิที่ความดันสุญญากาศ จะได้วัตถุดิบสำหรับผลิตเป็นน้ำมันหล่อลื่นพื้นฐาน 3 ชนิด ซึ่งน้ำมันที่ได้จะถูกส่งไปเก็บไว้ในถังสำรอง เพื่อส่งต่อไปยังหน่วยผลิตน้ำมันหล่อลื่นพื้นฐานต่อไป

1 หน่วยแยกแอสฟัลท์ (Propane Deasphalting Unit) ทำหน้าที่แยกกากน้ำมันจากหอกลั่นสุญญากาศโดยใช้โพรเพน เป็นตัวทำละลาย ซึ่งจะได้เป็นวัตถุดิบสำหรับการผลิตเป็นน้ำมันหล่อลื่นพื้นฐาน ชนิด 150 ไบรท์สต็อก และส่วนที่เหลือจากวัตถุดิบดังกล่าว สามารถนำไปผลิตยางมะตอยสำหรับการใช้ในการก่อสร้างถนนต่อไป

2 หน่วยสกัดสารอะโรเมติก (MP Refining Unit) ทำหน้าที่สกัดสารอะโรเมติก ออกจากวัตถุดิบสำหรับผลิตน้ำมันหล่อลื่นพื้นฐาน ที่ได้จากหน่วยกลั่นสุญญากาศและหน่วยแยกแอสฟัลท์ โดยใช้สารละลายที่เรียกว่า n-methly-2-pyrrolidone (NMP)เป็นตัวทำละลาย ซึ่งเป็นสารที่มีประสิทธิภาพสูง สามารถย่อยสลายในธรรมชาติได้ง่าย มีความเสถียรต่อความร้อน และการเข้าทำปฏิกิริยากับออกซิเจนสูงขึ้น น้ำมันที่ผ่านจากหน่วยนี้จะมีดัชนีความหนืดสูงขึ้น (ดังรูป 1.3)

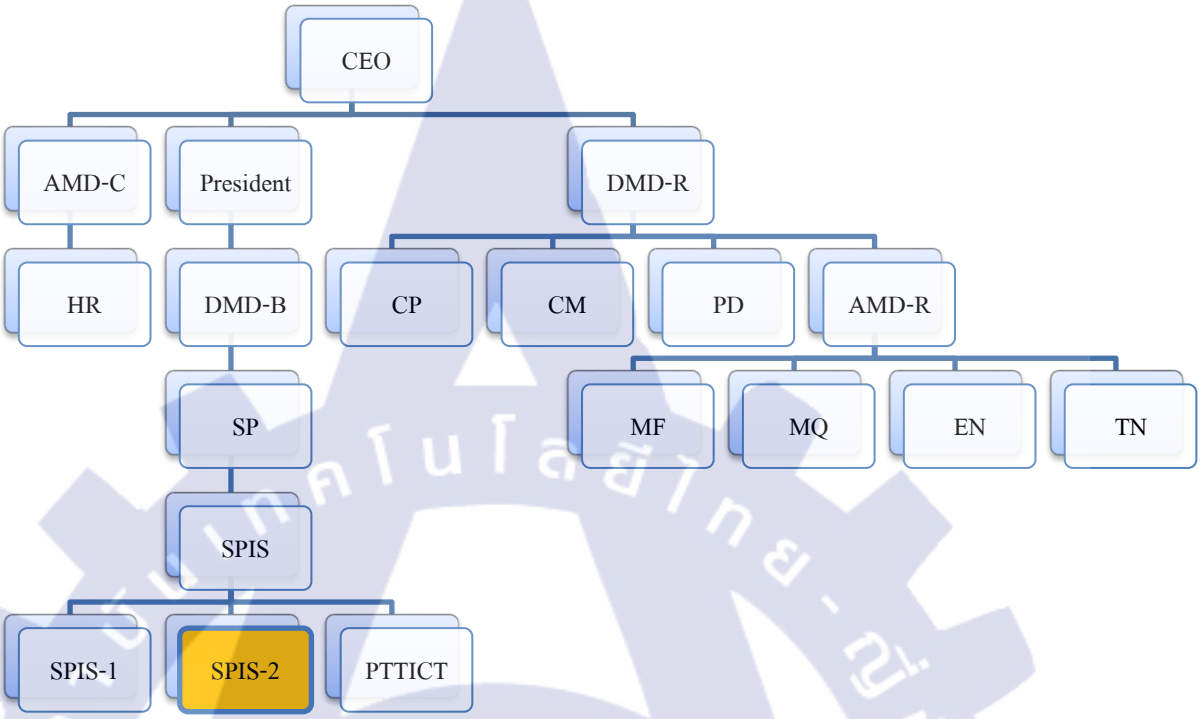
2.2 หน่วยกำจัดกำมะถันและฟอกสี (Hydrofinishing Unit) ทำหน้าที่ในการแยกเอากำมะถันที่มีอยู่ในน้ำมันหล่อลื่นพื้นฐานออก โดยใช้ไฮโดรเจนและสารเร่งปฏิกิริยา น้ำมันที่ผ่านจากหน่วยนี้จะบริสุทธิ์ มีสีใสยิ่งขึ้น(ดังรูป 1.3)

2.3 หน่วยแยกไขพาราฟิน (Solvent Dewaxing Unit) ทำหน้าที่แยกไขพาราฟินออกจากน้ำมัน ทำให้ได้น้ำมันหล่อลื่นพื้นฐานที่มีจุดไหลเทต่ำ เป็นน้ำมันบริสุทธิ์ ได้มาตรฐานสากล พร้อมจำหน่ายเพื่อนำไปใช้งานต่อไป (ดังรูป 1.3)



รูปที่ 1.3 กระบวนการผลิต

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร



รูปที่ 1.4 แผนผังองค์กร

1.3.1 วิสัยทัศน์

บริษัทชั้นนำของภูมิภาคเอเชียแปซิฟิคในการดำเนินธุรกิจ น้ำมันหล่อลื่นพื้นฐานและผลิตภัณฑ์พิเศษ

1.3.2 พันธกิจ

1) ผลิตและพัฒนาน้ำมันหล่อลื่นพื้นฐานและผลิตภัณฑ์พิเศษให้มีคุณค่าสูงสุด สอดคล้องกับความต้องการของตลาดที่เปลี่ยนแปลงไป

2) ดำเนินธุรกิจร่วมกับคู่ค้าโดยถือเสมือนหุ้นส่วน เพื่อเพิ่มผลประโยชน์และความสามารถในการแข่งขันร่วมกัน

3) ยึดมั่นในระบบคุณภาพ ความปลอดภัย อาชีวอนามัย และสิ่งแวดล้อม

4) ดำเนินธุรกิจด้วยความโปร่งใสและมีจริยธรรม

5) ส่งเสริมให้พนักงานทำงานเป็นทีม และมีส่วนร่วมในการพัฒนาองค์กร รวมทั้งมุ่งพัฒนาพนักงานเพื่อความเป็นเลิศในวิชาชีพ

1.3.3 ค่านิยมองค์กร

หลักการที่ไทยลู้บเบส ยึดมั่นเป็นหัวใจสำคัญของการพัฒนาองค์กร และเป็นคุณค่าที่มุ่งปลูกฝังแก่พนักงานทุกคน เพื่อพัฒนาองค์กรไปสู่วัฒนธรรมองค์กรที่ดีงาม แนวทางที่ไทยลู้บเบสยึดถือปฏิบัติได้แก่ C+ POSITIVE ซึ่งมีความหมายดังนี้

1) C = Customer Oriented (การมุ่งเน้นความพึงพอใจของลูกค้าผู้รับบริการหรือผู้มาติดต่อ มีความตั้งใจในการให้บริการ ช่วยเหลือ เสริมสร้างและรักษาความสัมพันธ์อันดีกับลูกค้าผู้รับบริการ หรือผู้มาติดต่อ ทั้งภายในและภายนอกองค์การ เข้าใจความต้องการและความคาดหวัง สามารถกำหนดแนวทางการปฏิบัติงานที่สอดคล้องและสนองความต้องการของลูกค้า ผู้รับบริการหรือผู้มาติดต่อให้เกิดความพึงพอใจ

2) P= Professionalism (ทำงานอย่างมืออาชีพ) มีแนวความคิด ความรู้ ความสามารถ ความเชี่ยวชาญ และทักษะในงานที่รับผิดชอบ แสวงหาความรู้เพื่อพัฒนาตนเองอย่างต่อเนื่องไปสู่การเป็นองค์กรแห่งการเรียนรู้ และยกระดับมาตรฐานการทำงานของตน ให้มีความเป็นเลิศในวิชาชีพและตอบสนองความต้องการทางธุรกิจขององค์กร

3) O = Ownership and Commitment (มีความรัก ผูกพัน และเป็นเจ้าขององค์กร) คิดเสมอว่าตนเป็นเจ้าของไทยลู้บเบส รัก ผูกพัน ร่วมมีส่วนได้ส่วนเสีย จึงทุ่มเททำงานอย่างเสียสละและเต็มความสามารถ เพื่อรักษาประโยชน์ สร้างความเจริญก้าวหน้า และความมั่นคงให้แก่องค์กร

4) S = Social Responsibility (ความรับผิดชอบต่อสังคม) ดำเนินธุรกิจอย่างเป็นมิตรต่อสิ่งแวดล้อม (Environmental Friendly) ดูแลรักษาและรับผิดชอบต่อครอบครัว เสริมสร้างความสัมพันธ์อันดีและมีส่วนร่วมในการพัฒนาชุมชนและสังคมให้มั่นคงและยั่งยืน

5) I = Integrity (ความซื่อสัตย์และยึดมั่นในความถูกต้องเป็นธรรม) ตั้งมั่นในความซื่อสัตย์สุจริต เป็นธรรม และโปร่งใส ในการทำธุรกิจ และปฏิบัติหน้าที่ภายใต้กรอบของระเบียบวินัย คุณธรรมและจริยธรรม เพื่อให้เกิดประโยชน์ร่วมกันกับเพื่อนร่วมงานลูกค้า คู่ค้า และผู้มีส่วนได้เสียทุกฝ่าย

6) T = Teamwork and Collaboration (ความร่วมมือทำงานเป็นทีม) ทำงานแบบร่วมมือเป็นทีม สามัคคี มีน้ำใจ รับฟังความคิดเห็นและสนับสนุนซึ่งกันและกัน ยึดเป้าหมายของทีมและองค์กรเป็นหลัก แก้ปัญหาความขัดแย้ง โดยยึดมั่นในสิ่งที่ถูกต้อง และพร้อมเสียสละเพื่อให้เกิดผลดีที่สุดต่อส่วนรวมและต่อทุกฝ่ายที่เกี่ยวข้อง

7) I = Initiative (ความริเริ่มสร้างสรรค์) มองหาโอกาส และริเริ่มในการสร้างสรรค์ ปรับปรุง และพัฒนาแนวความคิด วิธีการทำงาน ผลงาน ตลอดจนสิ่งใหม่ ๆ ให้สอดคล้องกับสภาวะแวดล้อมทางธุรกิจที่เปลี่ยนแปลงตลอดเวลา เพื่อเพิ่มมูลค่า (Add Value) ให้แก่งานของตนเองและแก่องค์กร อย่างต่อเนื่อง

8) V = Vision Focus (การมุ่งมั่นในวิสัยทัศน์) มุ่งมั่นที่จะดำเนินการให้บรรลุเป้าหมาย โดยยึดวิสัยทัศน์และพันธกิจขององค์กรเป็นหลัก และมีการเตรียมการเพื่ออนาคตอย่างจริงจัง และเป็นรูปธรรม

9) E = Excellence Striving (การมุ่งมั่นสู่ความเป็นเลิศ) ผลักดันตนเองและองค์กรสู่ความเป็นเลิศ ให้มีคุณภาพ ความปลอดภัย ประสิทธิผล และประสิทธิภาพที่ดีกว่า อย่างต่อเนื่องในทุก ๆ ด้าน เมื่อเทียบกับองค์กรชั้นนำระดับสากล

1.3.4 ระบบการจัดการ

ระบบบริหารคุณภาพ ความปลอดภัย อาชีวอนามัย สิ่งแวดล้อม บริษัทไทยลู้บเบส จำกัด (มหาชน) ได้พัฒนาระบบบริหารงานคุณภาพและการเพิ่มผลผลิต (TQP System-Thailube Quality and Productivity System) โดยเริ่มจากการนำมาตรฐาน ISO 9001 มาใช้ และได้รับการรับรองในปี 2541 ซึ่งต่อมาได้นำมาตรฐาน ISO 14001 และ TIS18001/OHSAS18001 ซึ่งเป็นเครื่องมือคุณภาพเข้ามาใช้ในบริษัทฯ อย่างต่อเนื่อง ได้แก่ กิจกรรม 5ส กิจกรรมข้อเสนอแนะและ QCC การวัดผลการดำเนินขององค์กรด้วยระบบ BSC&KPIs ระบบธรรมาภิบาล (CG) ระบบประเมินความเสี่ยงทั่วทั้งองค์กร (ERM) ค่านิยมองค์กร (C+POSITIVE) เกณฑ์รางวัลคุณภาพแห่งชาติ (TQA) เกณฑ์ความสำนึกรับผิดชอบต่อสังคม (CSR) และระบบการจัดการองค์ความรู้ (KM) กิจกรรมข้างต้น บริษัทฯ ได้ดำเนินการตามหลักการ PDCA (Plan-Do-Check-Action) ซึ่งพนักงานได้เรียนรู้ และนำไปใช้ในการปรับปรุงกระบวนการทำงานอย่างเป็นระบบ อันจะนำไปสู่การสร้างคุณค่าให้กับผู้มีส่วนได้ส่วนเสียขององค์กรอย่างยั่งยืน

1.3.5 การกำกับกิจการการดูแลที่ดี

บริษัท ไทยลู้บเบส จำกัด (มหาชน) มีเจตนารมณ์ในการดำเนินธุรกิจของบริษัทฯให้มีความโปร่งใส มีจริยธรรม มีความรับผิดชอบต่อผู้ที่มีส่วนได้ส่วนเสีย รวมทั้งคำนึงถึงสังคมและสิ่งแวดล้อมเป็นสำคัญ โดยการให้ความมั่นใจกับทุกฝ่ายว่าคณะกรรมการของบริษัทฯ ผู้บริหาร ตลอดจนพนักงานทุกคนจะยึดมั่นในความเป็นธรรม ปฏิบัติต่อผู้มีส่วนได้ส่วนเสียอย่างเท่าเทียมกัน และมีการดำเนินงานเพื่อผลประโยชน์ของบริษัทฯ อย่างเต็มความสามารถด้วยความสุจริต โปร่งใส

สามารถตรวจสอบได้ เพื่อให้บริษัทฯ สามารถบรรลุเป้าหมายข้างต้น และดำรงรักษาความเป็นเลิศในคุณธรรม อันเป็นคุณค่าพื้นฐานขององค์กร บริษัทฯ จึงได้จัดทำหลักการกำกับดูแลกิจการที่ดี (Good Corporate Governance Principles) ขึ้นเพื่อให้คณะกรรมการบริษัทฯ ผู้บริหาร และพนักงานของบริษัทฯ ทุกคน ยึดถือเป็นหลักปฏิบัติในการดำเนินงานด้วยมาตรฐานสูงสุด โดยถือเป็นภาระหน้าที่ที่สำคัญของทุกคน และจะต้องไม่ละเลยการปฏิบัติตามหลักการที่กำหนดขึ้น ส่วนหนึ่งที่สำคัญของหลักการนี้ประกอบด้วยปรัชญา และอุดมการณ์ในการดำเนินธุรกิจ จรรยาบรรณของคณะกรรมการบริษัทฯ และผู้บริหาร ข้อพึงปฏิบัติของพนักงาน รวมทั้งนโยบายที่สำคัญต่าง ๆ อันเป็นหลักการที่จะนำไปสู่การกำกับดูแลกิจการที่ดี คณะกรรมการ บริษัทฯ มีความเชื่อมั่นและศรัทธาต่อหลักปฏิบัติที่กล่าวถึงในหลักการกำกับดูแล กิจการที่ดี อย่างเต็มเปี่ยม บริษัทฯจะประสบความสำเร็จในการดำเนินธุรกิจอย่างยั่งยืน และสง่างามได้ ขึ้นอยู่กับบุคลากรในบริษัทฯ ทุกระดับ ที่จะต้องมีความเข้าใจและยึดมั่นปฏิบัติตามหลักการดังกล่าว อย่างต่อเนื่องและจริงจัง เพื่อความเป็นเลิศขององค์กรตลอดไป

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย

ตำแหน่ง : นักศึกษาแผนก SPIS

หน้าที่ :

1. การทำรายการทรัพย์สินที่อยู่ในศูนย์คอมพิวเตอร์ (Data Center) การวิเคราะห์ระบบในศูนย์คอมพิวเตอร์ (Data Center) เพื่อป้องกันภัยคุกคาม
2. ที่เกิดกับศูนย์คอมพิวเตอร์ (Data Center)
3. ออกแบบวิธีการเก็บรักษาข้อมูล เช่น เอกสาร สื่อบันทึกข้อมูล เป็นต้น
4. การปรับห้อง ศูนย์คอมพิวเตอร์ (Data Center) ให้ได้มาตรฐานตาม ISO 27001
5. การจัดทำนโยบายความปลอดภัยใน ศูนย์คอมพิวเตอร์ (Data Center)

1.5 พนักงานที่ปรึกษา และ ตำแหน่งของพนักงานที่ปรึกษา

พนักงานที่ปรึกษา : นาย เอกพจน์ ชมภูศรี

ตำแหน่งของพนักงานที่ปรึกษา : ตำแหน่ง ICT Strategy Supervisor

1.6 ระยะเวลาที่ปฏิบัติงาน

ปฏิบัติงานตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2554 ถึง 30 กันยายน พ.ศ. 2554

1.7 วัตถุประสงค์หรือจุดมุ่งหมายของการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมายให้ปฏิบัติงานสหกิจศึกษา

1) เพื่อจัดทำนโยบายความมั่นคงปลอดภัยขององค์กรโดยนำกระบวนการ PDCAมาประยุกต์ใช้เพื่อเป็นแนวทางในการปฏิบัติ

2) เพื่อจัดทำมาตรฐาน และขั้นตอนปฏิบัติด้านการให้บริการระบบสารสนเทศให้สอดคล้องกับมาตรฐาน ISO27001

3) เพื่อตรวจสอบภัยคุกคามและช่องโหว่ต่าง ๆ ที่อาจเกิดความเสี่ยงต่อองค์กรได้

4) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตทั้งจากภายในและภายนอก

วัตถุประสงค์โดยรวมของโครงการนี้ก็คือการรวบรวมวิธีการเพื่อนำมาใช้ในการแก้ไขปัญหาความเสี่ยงทางด้านการรักษาความปลอดภัยของข้อมูลสารสนเทศที่เกิดขึ้นกับองค์กรซึ่งต่อไปนี้ องค์กร หมายถึง บริษัท ไทยลู้บเบส จำกัด (มหาชน)

1.8 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย

เนื่องจากองค์กรที่นามาใช้ในกรณีศึกษาเป็นองค์กรที่ดำเนินธุรกิจเกี่ยวกับพลังงาน เป็นองค์กรที่มีขนาดใหญ่ มีลูกค้าหลายระดับตั้งแต่ระดับทั่วไป จนถึงระดับองค์กรชั้นนำ โดยการให้บริการในการจำหน่ายพลังงาน เป็นธุรกิจหลักขององค์กรและมีระบบเทคโนโลยีสารสนเทศคอยสนับสนุนให้ธุรกิจดำเนินงานได้อย่างต่อเนื่อง ตลอด 24 ชั่วโมงต่อ หากระบบเทคโนโลยีสารสนเทศขององค์กรล้มเหลวจากภัยพิบัติโดยมนุษย์ หรือธรรมชาติ จากความตั้งใจของบุคคลหรือไม่ก็ตาม ล้วนเป็นสิ่งที่ยอมรับไม่ได้ ดังนั้น การเตรียมแผน เพื่อรับมือกับเหตุการณ์ที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ที่อาจเกิดขึ้นได้จึงเป็นสิ่งสำคัญ ปัจจุบันองค์กรยังไม่มีแผนรองรับเหตุการณ์ที่เป็นรูปธรรมชัดเจน จึงอาจเกิดความเสี่ยงทางด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ในองค์กรได้ เช่น ขั้นตอนในการปฏิบัติงานที่ผิดพลาด เนื่องจากความไม่ชัดเจนของการรองรับแผนปฏิบัติงาน ดังนั้นเพื่อให้การดำเนินธุรกิจขององค์กร เป็นไปได้อย่างต่อเนื่อง จึงเป็นเรื่องที่สมเหตุสมผล

ด้วยเหตุผลดังกล่าวที่กล่าวในข้างต้น โครงงานนี้จึงมุ่งดำเนินการวิเคราะห์ และจัดทำแนวทางในการทำแผนเพื่อวางกรอบการวางแผนรองรับสถานการณ์ฉุกเฉินและเหตุการณ์ที่ไม่คาดคิด ตามกรอบมาตรฐาน ISO27001 ในการจัดทำเพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นได้ในอนาคต

บทที่ 2 ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.1 ความเสี่ยงและการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงิน และการบริหาร ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 4 ระดับ คือ สูงมาก สูง ปานกลางและต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management) หมายถึง การบริหารปัจจัย และควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่างๆ เพื่อลดมูลเหตุของแต่ละโอกาสที่องค์กรจะเกิดความเสียหาย ให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมาย ทั้งในด้านกลยุทธ์การปฏิบัติตามกฎระเบียบ การเงิน และชื่อเสียงขององค์กรเป็นสำคัญ โดยได้รับการสนับสนุนและการมีส่วนร่วมในการบริหารความเสี่ยงจากหน่วยงานทุกระดับทั่วทั้งองค์กร

การควบคุม (Control) หมายถึง นโยบาย แนวทาง หรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจพบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

2.2 นโยบายความมั่นคงปลอดภัย (Security policy)

การกำหนดจัดทำมาตรฐานนโยบายด้านความมั่นคงปลอดภัยที่เกี่ยวกับสารสนเทศสำหรับองค์กร ที่ต้องสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่จัดทำเป็นนโยบายลายลักษณ์อักษรที่ได้รับอนุมัติจากผู้บริหารขององค์กร เพื่อเผยแพร่ให้องค์กรและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบ

2.2.1 โครงสร้างด้านความมั่นคงปลอดภัยในองค์กร (Organization of Information Security)

โครงสร้างด้านความมั่นคงปลอดภัยในองค์กร (Internal organization) การบริหารและจัดการด้านความมั่นคงปลอดภัยสารสนเทศในองค์กร มีดังนี้

1) การให้ความสำคัญสนับสนุนการบริหารจัดการด้านความมั่นคงปลอดภัย (Management Commitment to Information Security) ที่มีข้อกำหนดที่ชัดเจน และการปฏิบัติที่สอดคล้องกับการมอบหมายงานที่เหมาะสมกับบุคลากร ที่เป็นหน้าที่ความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

2) การประสานงานร่วมมือกันในการสร้างความมั่นคงปลอดภัยสารสนเทศขององค์กรโดยการกำหนดตัวแทนบุคลากรขององค์กรในการสร้างความมั่นคงปลอดภัยสารสนเทศ

3) การกำหนดหน้าที่ความรับผิดชอบของบุคลากรในการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

4) การกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ

5) การจัดให้มีการลงนามข้อตกลงระหว่างบุคลากรกับองค์กรมิให้เปิดเผยความลับขององค์กร

6) การกำหนดรายชื่อและข้อมูลสำหรับการติดต่อประสานงานกับหน่วยงานอื่นด้านความมั่นคงปลอดภัยในกรณีที่จำเป็น

7) การกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับกลุ่มต่าง ๆ ที่มีความสนใจเป็นพิเศษในกลุ่มด้านความมั่นคงปลอดภัยสารสนเทศ

8) การกำหนดให้มีการตรวจสอบการบริหารจัดการดำเนินงาน การปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ โดยผู้ตรวจสอบอิสระเป็นผู้ตรวจสอบตามรอบระยะเวลาที่มีกำหนดไว้

หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญกับองค์กร โครงสร้างด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties) การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรที่ถูกเข้าถึงถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

9) การกำหนดให้มีการประเมินความเสี่ยงที่เกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก

10) การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กร

11) การระบุข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่มีความจำเป็นสำหรับความมั่นคงปลอดภัยขององค์กร ระหว่างองค์กรและหน่วยงานภายนอก

2.2.2 การบริหารจัดการทรัพย์สิน (Asset management)

การกำหนดหน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) การจัดทำบัญชีทรัพย์สิน (Inventory of assets) การจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ การระบุผู้เป็นเจ้าของทรัพย์สินที่เป็นส่วนสารสนเทศ (Ownership of assets) ตามที่กำหนดไว้ในบัญชีทรัพย์สิน การจัดทำกฎระเบียบหรือหลักเกณฑ์ที่เป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศ และทรัพย์สินที่เกี่ยวกับการประมวลผลสารสนเทศอย่างเหมาะสม

2.2.3 ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

การกำหนดบริเวณที่ต้องรักษาความมั่นคงปลอดภัยโดยการป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต เป็นการก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร การจัดทำบริเวณความมั่นคงปลอดภัย มีดังนี้

1) การจัดทำบริเวณล้อมรอบ เป็นการจัดสรรพื้นที่ กั้นบริเวณการเข้า – ออกของสำนักงานองค์กร โดยมีหน่วยรักษาความปลอดภัยควบคุมการผ่านเข้า - ออก เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

2) การควบคุมการเข้า – ออก ในบริเวณพื้นที่ที่ต้องการรักษาความปลอดภัยต้องอนุญาตให้ผ่าน เข้า – ออก ได้เฉพาะผู้ได้รับอนุญาตเท่านั้น ที่เป็นการรักษาความมั่นคงปลอดภัยสำหรับสำนักงานขององค์กร และทรัพย์สิน

3) การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การ ระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่น ๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

4) การจัดให้มีการป้องกันทางกายภาพสำหรับการปฏิบัติงานในพื้นที่ ที่ต้องรักษาความมั่นคง ปลอดภัย

5) การจัดบริเวณสำหรับการเข้าถึงเทคโนโลยีสารสนเทศ หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กร โดยไม่ได้รับอนุญาตการจัดบริเวณควรจัดแยกออกมาต่างหากตามความเหมาะสม

2.3 มาตรฐานด้านความมั่นคงปลอดภัย

1) มาตรฐาน ISO27001 เป็นมาตรฐานสากลมุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร และใช้เป็นมาตรฐานอ้างอิงเพื่อเป็นแนวทางในการเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรอย่างแพร่หลาย

2) มาตรฐาน Cobit (Control Objective for Information and Related Technology) ถูกพัฒนาขึ้นโดยกลุ่มความร่วมมือที่ชื่อว่า “ISACA” ใช้สำหรับองค์กรที่ต้องการมุ่งสู่การเป็น “ไอทีภิบาล” หรือ “IT Governance” กำลังเป็นที่นิยมในกลุ่มธุรกิจด้านการเงินและการธนาคารยกตัวอย่าง เช่น ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ เป็นต้น

3) มาตรฐาน ITIL (IT Infrastructure Library)/BS15000 กล่าวถึง "Best Practice” ในการบริหารจัดการงานให้บริการด้านระบบสารสนเทศ เช่น มาตรฐานด้าน Service Support และService Delivery ตลอดจน การกำหนด SLA (Service Level Agreement) เป็นต้น

2.3.1 มาตรฐานที่เลือกใช้

มาตรฐาน ISO27001 เป็นมาตรฐานเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ ซึ่งจะกำหนดความต้องการ (Set of Requirements) เกี่ยวกับการจัดทำระบบให้มีความมั่นคงปลอดภัย ซึ่งมีวัตถุประสงค์เพื่อช่วยให้องค์กรสามารถสร้างระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศขึ้นมาได้อย่างมีประสิทธิภาพ ทั้งนี้ มาตรฐานดังกล่าวสามารถนำมาใช้ได้กับทุก ๆ ประเภทขององค์กรที่เกี่ยวข้องกับความมั่นคงปลอดภัย ไม่ว่าจะเป็นองค์กรขนาดใหญ่หรือขนาดย่อมก็ตาม

ระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ เป็นส่วนหนึ่งในระบบบริหารจัดการขององค์กร ซึ่งมีพื้นฐานมาจากแนวทางการจัดการความเสี่ยงของธุรกิจ (Business Risk Approach)

มีวัตถุประสงค์เพื่อรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศ (Information) รวมทั้งทรัพย์สินอื่น ๆ ที่มีความสำคัญขององค์กร ในการที่จะสร้าง ดำเนินการ นำมาใช้ ตรวจสอบ วัดผลทบทวน บำรุงรักษาและปรับปรุงระบบบริหารความมั่นคงปลอดภัย เพื่อให้องค์กรลดความเสี่ยงจากภัยคุกคามต่าง ๆ โดยใช้หลัก Plan-Do-Check-Act (PDCA Model)

มาตรฐาน ISO27001 โดยสรุปเนื้อหาแบ่งออกเป็น 11 โดเมน (Domain) ซึ่งแต่ละโดเมนประกอบด้วยวัตถุประสงค์แตกต่างกัน รวมแล้วจำนวน 39 วัตถุประสงค์ (Control objectives) และภายใต้วัตถุประสงค์แต่ละข้อประกอบด้วยมาตรการในการรักษาความมั่นคงปลอดภัยแตกต่างกัน รวมแล้ว 133 ข้อ (Controls) สามารถนำไปประยุกต์ใช้เพื่อรักษาความมั่นคงให้กับระบบสารสนเทศขององค์กร ซึ่ง 11 หมวดหลักที่ครอบคลุมโดยมาตรฐาน ISO 27001 ได้แก่

1) Security policy ครอบคลุมเรื่องนโยบายการจัดการความมั่นคงของข้อมูลในองค์กร เล็งเห็นถึงความสำคัญของนโยบายฯ และการให้การสนับสนุนจากผู้บริหารระดับสูงเพื่อให้มีการนำนโยบายไปใช้อย่างมีประสิทธิภาพ

2) Organizational of information security ครอบคลุมเรื่องการจัดตั้งหน่วยงานขึ้นเพื่อประสานงานและดำเนินงานด้านการดูแลรักษาความมั่นคงของข้อมูล ตลอดจนการบริหารจัดการด้านความมั่นคงของข้อมูลภายในองค์กร และการประสานงานทั้งภายในและภายนอกองค์กร

3) Asset management ครอบคลุมเรื่องการจัดทำทะเบียนทรัพย์สิน การจัดจำแนกประเภทของข้อมูลตามระดับความสำคัญ การควบคุมการเข้าถึงข้อมูลแต่ละประเภท และการควบคุมทรัพย์สินด้านสารสนเทศขององค์กร

4) Human resources security ครอบคลุมเรื่องการบริหารจัดการความมั่นคงในส่วนที่เกี่ยวข้องกับพนักงาน และผู้วิจัย ตั้งแต่เริ่มรับพนักงานใหม่ จวบจนสิ้นสุดสถานภาพการเป็นพนักงาน ซึ่งครอบคลุมประเด็นที่สำคัญต่าง ๆ อาทิเช่น การให้ความรู้ด้านความมั่นคงแก่พนักงาน การให้พนักงานลงนามในข้อตกลงไม่เปิดเผยข้อมูล เป็นต้น

5) Physical and environmental security ครอบคลุมเรื่องการรักษาความมั่นคงของสถานที่ทำงาน ได้แก่การควบคุมการเข้า-ออกของบุคคล และทรัพย์สิน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและป้องกันการเสียหายหรือสูญหายของทรัพย์สิน

6) Communications and operations management ครอบคลุมเรื่องการรักษาความมั่นคงให้แก่คอมพิวเตอร์ ระบบเครือข่าย และการประมวลผลข้อมูล เช่น การป้องกันไวรัสคอมพิวเตอร์ การสำรองข้อมูล การควบคุมความมั่นคงของระบบเครือข่าย การกำจัดสื่อบันทึกข้อมูล การควบคุมความมั่นคงในการใช้งานอีเมล์ ฯลฯ

7) Access control ครอบคลุมเรื่องการควบคุมการเข้าถึงข้อมูล และการป้องกันการเข้าถึงข้อมูลโดยผู้ไม่ได้รับอนุญาตทั้งจากการเข้าใช้งานภายในองค์กร และการเข้าถึงระบบจากระยะไกล (Remote access)

8) Information systems acquisition, development and maintenanceครอบคลุมเรื่องการจัดซื้อ-จัดหา พัฒนา ติดตั้ง และบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย ซอฟต์แวร์ ฮาร์ดแวร์ และอุปกรณ์สารสนเทศต่าง ๆ เพื่อให้อุปกรณ์เหล่านั้นมีความมั่นคงและทำงานได้อย่างมีประสิทธิภาพ

9) Information security incident management ครอบคลุมเรื่องการรายงาน และการบริหารจัดการเหตุละเมิดความมั่นคงของข้อมูล เพื่อให้เหตุดังกล่าวได้รับการแก้ไขอย่างทันท่วงที และป้องกันไม่ให้เกิดเหตุซ้ำขึ้นอีกในอนาคต

10) Business continuity management ครอบคลุมเรื่องการจัดทำและทดสอบแผนความต่อเนื่องในการดำเนินธุรกิจ (Business continuity Plan หรือ BCP) ซึ่งก็คือวิธีปฏิบัติในการรับมือสำหรับกรณีที่เกิดความผิดพลาดขึ้นกับระบบสารสนเทศ หรือภัยธรรมชาติ เพื่อให้เกิดความเสียหายน้อยที่สุดและเพื่อให้ธุรกิจสามารถฟื้นตัวกลับมาดำเนินงานตามปกติได้เร็วที่สุด

11) Compliance ครอบคลุมการปฏิบัติงานที่ถูกต้องตามกฎหมาย หรือข้อตกลงต่าง ๆ ที่องค์กรได้กระทำร่วมกับผู้อื่น เช่น การใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ (License) ถูกต้อง การปกป้องข้อมูลส่วนบุคคล ฯลฯ

อย่างไรก็ตามมาตรฐาน ISO27001 นี้ถูกออกแบบมาสำหรับการตรวจประเมิน (Certification) นั่นคือถ้าองค์กรใดได้จัดทำระบบตามมาตรฐานนี้ครบถ้วนตามความต้องการที่กำหนดไว้แล้ว องค์กรดังกล่าวสามารถยื่นคำขอไปยังหน่วยงานรับตรวจประเมินระบบ (Certification Body) เพื่อให้เข้ามาดำเนินการตรวจประเมินและรับรองระบบที่จัดทำขึ้นได้ แต่อย่างไรก็ตาม ความซับซ้อนของระบบบริหารความมั่นคงปลอดภัยของสารสนเทศที่แต่ละองค์กรพัฒนาขึ้นจะมีความแตกต่างกันไป ขึ้นอยู่กับ ขนาด โครงสร้าง วัตถุประสงค์ ความต้องการเกี่ยวกับความมั่นคงปลอดภัย รวมไปถึงกระบวนการทางธุรกิจ (Business Processes) ขององค์กร

2.3.2 ประโยชน์จากการใช้มาตรฐาน ISO27001

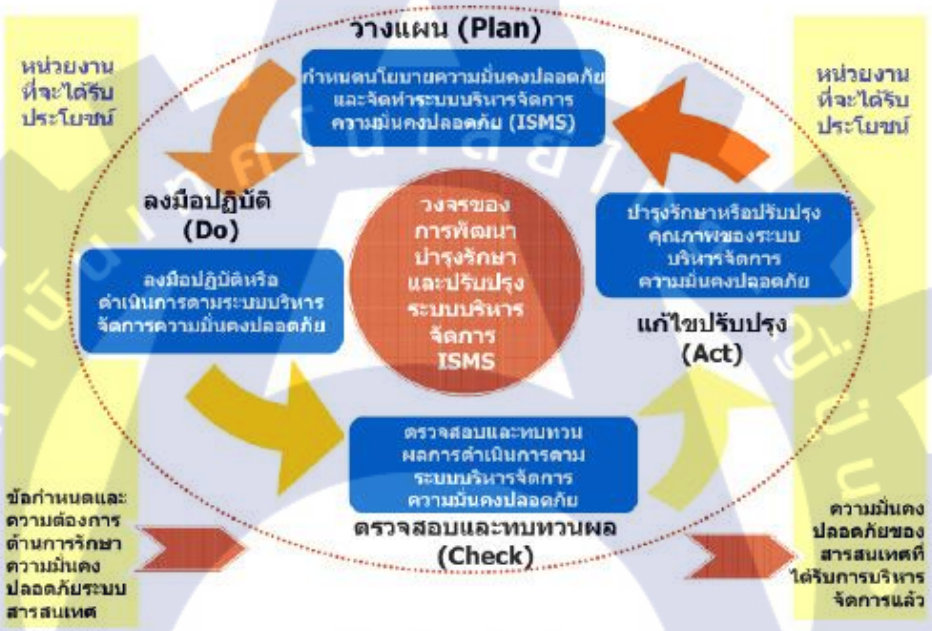
1) เนื่องจาก การมีข้อมูลและระบบการจัดเก็บข้อมูล ที่มีความปลอดภัยเที่ยงตรงและพร้อมใช้งานเสมอนั้นย่อมช่วยสร้างความได้เปรียบทางการแข่งขัน สร้างผลกำไร และสร้างโอกาสทางการธุรกิจ

2) สอดคล้องกับกฎหมาย ตามพระราชบัญญัติ

3) สร้างความมั่นใจให้กับบริษัทคู่ค้ารับประกันความต่อเนื่องในการทำธุรกิจระหว่างคู่ค้า

4) จากการประเมินความเสี่ยง การแยกแยะภัยคุกคามของข้อมูล การรับรู้จุดอ่อนและความเป็นไปได้ของความเสี่ยง และ จากการพิจารณาอย่างถี่ถ้วนของผลกระทบที่จะเกิดนี่เองย่อมเป็นผลดีกับธุรกิจท่านในการเลือกลงทุนที่จะก่อประโยชน์และคุ้มค่าที่สุด

2.4 PDCA (Plan-Do-Check-Act)



รูปที่ 2.1 ระบบการทำงาน PDCA

PDCA (Plan-Do-Check-Act) เป็นกิจกรรมพื้นฐานในการพัฒนาประสิทธิภาพและคุณภาพของการดำเนินงาน ซึ่งประกอบด้วย ขั้นตอน 4 ขั้น คือ วางแผน (Plan) - ปฏิบัติ (Do) - ตรวจสอบ (Check) – ปรับปรุงการดำเนินกิจกรรม (Act) PDCA อย่างเป็นระบบให้ครบวงจรอย่างต่อเนื่องหมุนเวียนไปเรื่อย ๆ ย่อมส่งผลให้การดำเนินงานมีประสิทธิภาพและมีคุณภาพ

2.4.1 วางแผน (Plan)

หมายความรวมถึงการกำหนดเป้าหมายหรือวัตถุประสงค์ในการดำเนินงานวิธีการ และขั้นตอนที่จำเป็นเพื่อให้การดำเนินงาน บรรลุเป้าหมายในการวางแผนจะต้องทำความเข้าใจกับ

เป้าหมาย วัตถุประสงค์ให้ชัดเจน เป้าหมายที่กำหนดต้องเป็นไปตามนโยบาย วิสัยทัศน์และพันธกิจขององค์กรเพื่อก่อให้เกิดการพัฒนาที่เป็นไปในแนวทางเดียวกันทั่วทั้งองค์กร การวางแผนในบางด้านอาจจำเป็นต้องกำหนดมาตรฐาน ของวิธีการทำงานหรือ เกณฑ์มาตรฐานต่าง ๆ ไปพร้อมกันด้วยข้อกำหนดที่เป็นมาตรฐานนี้ จะช่วยให้การวางแผนมีความสมบูรณ์ยิ่งขึ้น เพราะใช้เป็นหลักเกณฑ์ในการตรวจสอบได้ว่า การปฏิบัติงานเป็นไปตามมาตรฐานที่ได้ระบุไว้ในแผนหรือไม่ Establish ISMS ได้แก่

1) กำหนด scope และ ขอบเขตการจัดทำระบบ ISMS
2) กำหนด ISMS Policy
3) กำหนด รูปแบบการประเมินความเสี่ยง
4) กำหนดความเสี่ยง
5) วิเคราะห์ และ ประเมินความเสี่ยง
6) กำหนดและประเมิน วิธีการเพื่อลดความเสี่ยง
7) เลือกการควบคุม เพื่อลดความเสี่ยง
8) เห็นชอบความเสี่ยงที่เหลืออยู่โดย management
9) เห็นชอบและประยุกต์ใช้ ระบบ โดย management
10) จัดทำ Statement of Applicable (SOA)

2.4.2 ปฏิบัติ (DO)

เป็นการปฏิบัติให้เป็นไปตามแผนที่ได้กำหนดไว้ ซึ่งก่อนที่จะปฏิบัติงานใด ๆ จำเป็นต้องศึกษาข้อมูลและเงื่อนไขต่าง ๆ ของ สภาพงานที่เกี่ยวข้องเสียก่อน ในกรณีที่เป็นงานประจำที่เคยปฏิบัติหรือเป็นงานเล็กอาจใช้วิธีการเรียนรู้ ศึกษาค้นคว้าด้วยตนเอง แต่ถ้าเป็นงานใหม่หรืองานใหญ่ที่ต้องใช้บุคลากรจำนวนมากอาจต้องจัดให้มีการฝึกอบรม ก่อนที่จะปฏิบัติจริงการปฏิบัติจะต้องดำเนินการไปตามแผน วิธีการ และขั้นตอน ที่ได้กำหนดไว้และจะต้องเก็บรวบรวมและบันทึก ข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานไว้ด้วยเพื่อใช้เป็นข้อมูลในการดำเนินงานในขั้นตอนต่อไป Implement and Operate the ISMS ได้แก่

1) กำหนดแผนการลดความเสี่ยง
2) ดำเนินการตามแผนลดความเสี่ยง
3) ดำเนินการ ตามการควบคุมที่เลือกตาม Plan
4) กำหนดการวัดประสิทธิภาพของระบบการควบคุม
5) จัดทำรายการฝึกอบรม

6) จัดการการประยุกต์ใช้ระบบ

7) ประยุกต์ใช้ ระเบียบปฏิบัติงาน

2.4.3 ตรวจสอบ (Check)

เป็นขั้นตอนที่มีขึ้นเพื่อประเมินผลว่ามีการปฏิบัติงานตามแผน หรือไม่มีปัญหาเกิดขึ้นในระหว่างการปฏิบัติงานหรือไม่ ขั้นตอนนี้มีความสำคัญ เนื่องจากในการดำเนินงานใด ๆ มักจะเกิดปัญหาแทรกซ้อนที่ทำให้การดำเนินงานไม่เป็นไปตามแผนอยู่เสมอ ซึ่งเป็นอุปสรรค ต่อประสิทธิภาพและคุณภาพของการทำงาน การติดตามการตรวจสอบ และการประเมินปัญหาจึงเป็นสิ่งสำคัญที่ต้องกระทำควบคู่ไปกับการดำเนินงาน เพื่อจะได้ทราบข้อมูลที่เป็นประโยชน์ในการปรับปรุงคุณภาพ ของการดำเนินงานต่อไปในการตรวจสอบ และการประเมินการปฏิบัติงานจะต้องตรวจสอบด้วย ว่าการปฏิบัตินั้น เป็นไปตามมาตรฐานที่กำหนดไว้หรือไม่ทั้งนี้เพื่อเป็นประโยชน์ต่อการพัฒนาคุณภาพของงาน Monitor and review ISMS ได้แก่

1) จัดทำ ระเบียบปฏิบัติการ เฝ้าระวังและตรวจสอบระบบ ISMS

2) ทบทวนประสิทธิภาพของ ระบบอย่างสม่ำเสมอ

3) วัดประสิทธิภาพการควบคุมในการปฏิบัติตามข้อกำหนด

4) ทบทวน การประเมินความเสี่ยงตามแผน ความเสี่ยงที่เหลือ ระบบการประเมินความเสี่ยง และการเปลี่ยนแปลงต่าง ๆ ตามรอบเวลาที่กำหนด

5) ดำเนินการ ตรวจติดตามภายในระบบ ISMS

6) ดำเนินการ จัดทำ Management Review

7) ปรับปรุง Security Plan ให้ทันสมัย

8) บันทึกการการทำงานและหลักฐานที่มีผลต่อประสิทธิภาพและประสิทธิผลของระบบ

2.4.4 การปรับปรุง (Act)

เป็นขั้นตอนที่มีขึ้นเพื่อแก้ไขปัญหาที่เกิดขึ้นหลังจากได้ทำการตรวจสอบแล้ว การปรับปรุงอาจเป็นการแก้ไขแบบเร่งด่วน เฉพาะหน้า หรือการค้นหาสาเหตุที่แท้จริงของปัญหาเพื่อป้องกันไม่ให้เกิดปัญหาซ้ำรอยเดิม การปรับปรุงอาจนำไปสู่การกำหนดมาตรฐานของวิธีการทำงานที่ต่างจากเดิมเมื่อมีการดำเนินงานตามวงจร PDCA ในรอบใหม่ข้อมูลที่ได้จากการปรับปรุงจะช่วยให้การวางแผนมีความสมบูรณ์และมีคุณภาพ เพิ่มขึ้นได้ด้วยการบริหารงานในระดับต่าง ๆ และแก้ไขปรับปรุงจุดที่เป็นปัญหาหรืออาจต้องปรับแผนใหม่ ในแต่ละปี เพื่อให้วิสัยทัศน์และแผน

ยุทธศาสตร์ระยะยาวนั้นปรากฏเป็นจริงและ ทำให้การดำเนินงานบรรลุเป้าหมายและวัตถุประสงค์รวมขององค์กร ได้อย่างมีประสิทธิภาพและมีคุณภาพ Maintain and improve the ISMS ได้แก่

1) ดำเนินการ corrective action และ preventive action
2) สื่อสาร วิธีการและการปรับปรุงต่าง ๆ ให้กับผู้ที่เกี่ยวข้องต่าง ๆ
3) แน่ใจว่า วิธีการที่ปรับปรุงขึ้น บรรลุจุดประสงค์ที่วางไว้

2.5 ภัยคุกคามในระบบเครือข่ายสารสนเทศ

2.5.1 Denial of Service Attack (DOS)

เป็นรูปแบบการโจมตีที่มีจุดประสงค์เพื่อการทำให้เครือข่ายหรือเซิร์ฟเวอร์ปฏิเสธการให้บริการหรือไม่สามารถดำเนินการต่อไปได้ลักษณะการโจมตีแบบนี้เป็นการทำให้เครือข่ายเต็มไปด้วยทราฟฟิก (Traffic) ขนาดมหาศาล ทำให้เกิด Connection จำนวนมากจนทำให้ระบบทำงานช้าลงหรืออาจล่มลงได้ การโจมตีในลักษณะนี้ไม่เพียงแต่ทำให้ เครือข่ายติดขัดเนื่องจากปริมาณทราฟฟิก (Traffic) ที่เพิ่มขึ้น แต่ยังมีการส่งแพ็คเกจพิเศษที่ถูก จัดทำขึ้นเพื่อให้โปรโตคอลการทำงาน ของเครื่องคอมพิวเตอร์เป้าหมายเกิดความสับสนหรือทำให้แอพพลิเคชั่นรวมทั้งการให้บริการต่าง ๆ บนเครื่องเป้าหมายหยุดทำงานหรือไม่สามารถทำงานต่อไปได้

2.5.2 ARP Poisoning

การดักจับข้อมูลบนเครือข่ายที่ใช้สวิตซ์นั้น เราไม่สามารถที่จะดักจับข้อมูลได้โดยตรง เนื่องจากสวิตซ์จะมีคุณสมบัติทางด้านความปลอดภัยที่ทำให้บุคคลที่สาม (ผู้บุกรุก) ไม่สามารถดักจับข้อมูลโดยใช้วิธีการทั่วไปได้ โดยผู้บุกรุกจะใช้วิธีการพิเศษที่สามารถดักจับข้อมูลที่วิ่งอยู่บนเครือข่ายที่ใช้สวิตซ์ได้ผู้บุกรุกจะใช้เทคนิคที่เรียกว่า ข้อมูล Man in the Middle เพื่อทำให้ตนเองเสมือนว่านั่งอยู่ตรงกลางระหว่างทางในการส่งการข้อมูลกันทำให้ผู้ที่เป็น Man in the Middle นั้นทำได้หลายวิธี แต่ที่นิยมกันโดยส่วนมากจะใช้วิธีการ ARP Poisoning กลไกลการทำงานของ ARP Poisoning การทำงานง่าย ๆ ของARP มี 2 ขั้นตอน คือ

1) เครื่องที่ต้องการสอบถาม MAC Address โดยการส่ง ARP Request ซึ่งประกอบด้วย MAC Address และ IP Address ของตนเอง และ IP Address ของเครื่องที่ต้องการทราบ MAC Address ส่วน MAC Address ปลายทางนั้น จะถูกกำหนดเป็น FF: FF:FF: FF: FF: FF ซึ่งเป็น Broadcast Address เพื่อให้ ARP Request ถูกส่งไปยังเครื่องที่อยู่ในเครือข่ายเดียวกัน

2) เครื่องที่มี IP Address ตรงกับที่ระบุใน ARP Request จะตอบกลับมาด้วยARP Reply ซึ่งประกอบด้วย MAC Address และ IP Address ของตนเองเป็นผู้ส่ง และใส่ MAC Address และ IP Address ของเครื่องที่ส่งมาเป็นผู้รับ ARP Reply สำหรับการโจมตีนั้น เครื่องที่โจมตีจะส่ง ARP Request โดยระบบ MAC Address ของ Gateway ที่ผิด ๆ ไป ทำให้เครื่องที่ถูกโจมตีนำ MAC Address ไปอัพเดต ARP Table และยัง ส่ง MAC Address ปลอมไปยังGateway ด้วยทำให้ Gateway อัพเดต ARP Table ที่ผิด เช่นกัน ส่งผลให้การ Broadcast ไปยังเครื่องต่าง ๆ ไม่ถูกต้องทำให้เครื่อง Client นั้น ๆ ไม่สามารถใช้งานระบบเครือข่ายได้ในที่สุด

2.6 เครื่องมือในการทดสอบระบบ

1) Super Scan โปรแกรมสแกนพอร์ตแบบฟรีแวร์ (Freeware) ที่นิยมใช้ในปัจจุบัน เนื่องจากตัวของโปรแกรม Super Scan เป็นโปรแกรมที่มีชื่อเสียงและจุดเด่นในด้านการสแกนพอร์ตได้อย่าง รวดเร็วและมีประสิทธิภาพ

2) Nmap (Network Mapping) เป็นโปรแกรม Open source ที่ใช้สแกนเครือข่าย และตรวจสอบ ความปลอดภัยซึ่ง Nmap ถูกพัฒนาให้สามารถทำการสแกนเครือข่ายขนาดใหญ่ ได้อย่างรวดเร็ว โดยการสแกน IP Address เพื่อที่จะรายงานพอร์ต แอพพลิเคชั่น ระบบปฏิบัติการและไฟร์วอลล์ ในปัจจุบัน Nmap มีให้ใช้งานทั้งแบบผ่านคำสั่งและแบบ Graphic GUI และทำงานได้บนระบบปฏิบัติการทุกประเภท หากผู้ใช้งานไม่ถนัด และจำรูปแบบคำสั่งไม่ได้ ก็มีให้เลือกใช้งานแบบ Graphic GUI ซึ่งไม่จำเป็นต้องจำคำสั่งต่าง ๆ

3) Nessus เป็นเครื่องมือสำหรับการตรวจสอบการบุกรุกซึ่งใช้สำหรับการสแกนช่องโหว่ Nessus สามารถแสดงรายงานออกมาว่าแต่ละเครื่องมีช่องโหว่อะไรบ้าง ระดับความเสี่ยงที่จะถูกโจมตีมี มาก-น้อย แค่ไหนวิธีป้องกันทำได้อย่างไรบ้าง

4) SQL Scan เป็นเครื่องมือสำหรับทำการตรวจสอบว่าเครื่องไหนบางภายในเครือข่ายได้ติดตั้ง โปรแกรม Microsoft SQL Server

5) SQL Dict เป็นเครื่องมือสำหรับถอดรหัส Microsoft SQL Server โดยเทียบจากคำศัพท์จากไฟล์ Dictionary

6) Pwdump3v2 เป็นเครื่องมือสำหรับดัมพ์เอารหัสผ่านจาก Registry ของเครื่อง เหยื่อออกมาเป็นไฟล์ Text

7) LC4 เป็นเครื่องมือสำหรับการถอดรหัสที่พัฒนาเพื่อใช้ในการอ่านไฟล์ SAM (Security Account Manager) ของ Windows ในตระกูล XP และ 2000 ทั้งที่ถูกเข้ารหัสแบบ SYSKEY และแบบธรรมดา

8) Cisco Password Decoder เป็นเครื่องมือสำหรับการถอดรหัสของอุปกรณ์ Cisco

2.7 รูปแบบการทำ Inventory Asset

ตารางที่ 2.1 Information Asset

		Asset Value										
No.	Information Detail	C	I	A	Risk Assessment Item	Classification	Format	Storage	Backup	Owner	Legal & Contract Related	Remark
1	Server Configuration	H	H	H	Configuration	Confidential	Electronics	File Server	Tape	SPIS		
2	Operation Manual (Paper)	M	M	M	Internal Document	Internal Use Only	Paper	Cabinet		SPIS		

ตารางที่ 2.2 Software Asset

		Asset Value											
No.	Software Detail	C	I	A	Risk Assessment Item	Type	No. of License	Expired date	SW Package (Manual/CD/Key)	Package Storage	Installed on	Owner	Legal & Contract Related	Remark
1	Windows Server 2000	M	M	H	Server OS	Commercial			CD & License	Phubai Office	Server	Thaioil	Copyright Act	

ตารางที่ 2.3 Physical Asset

No.	Physical Detail	Quantity	Asset Value			Risk Assessment Item	Location	Owner	Legal & Contract Related	Remark
			C	I	A					
1	Access Control Server - Windows 2000 - PRD	1	H	H	H	Main Server	Phubai Data Center	SPIS	Hardware MA	

ตารางที่ 2.4 Personnel Asset

No.	Personnel Detail	Type	Quantity	Asset Value			Risk Assessment Item	Owner	Legal & Contract Related	Remark
				C	I	A				
1	SPIS Manager	Normal	1	H	H	M	Manager	SPIS	Labour Law	

ตารางที่ 2.5 Service Asset

No.	Service Detail	Service Provider	Asset Value			Risk Assessment Item	Contact Name	Contact Tel.	Owner	Legal & Contract Related	Remark
			C	I	A						
1	Server Maintenance Dell	Dell	H	H	H	Machine MA			SPIS	Service Agreement	

ตารางที่ 2.6 Location Asset

No.	Location Detail	Address	Asset Value			Risk Assessment Item	Responsible Person	Remark
			C	I	A			
1	Office Phubai Building	42/1 Moo 1 Sukhumvit Road Km. 124, Tungsukla, Sriracha, Cholburi 20230, Thailand	M	M	M	Office(Phubai Building)	K. Yohan ,K. Eakapoj	

บทที่ 3 แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน

3.1 แผนงานในการปฏิบัติงาน

ตารางที่ 3.1 ระยะเวลาการปฏิบัติงาน

	รายละเอียดกิจกรรม	M1	M2	M3	M4	M5	M6	M7	M8
1	เริ่มต้นโครงการและจัดโครงสร้างคณะทำงาน								
2	จัดทำทะเบียนทรัพย์สินและประเมินความเสี่ยง								
3	วางแผนแก้ไขความเสี่ยงและกำหนดตัวชี้วัด								
4	ดำเนินการแก้ไขความเสี่ยงและวัดผล								
5	ทบทวน/ปรับปรุงนโยบายความมั่นคงปลอดภัยของสารสนเทศ และเอกสารสนับสนุน								
6	ทบทวน/ปรับปรุงแผนความต่อเนื่องในการดำเนินธุรกิจ								
7	ทบทวน/ปรับปรุงเอกสารกระบวนการของระบบ ISMS								
8	การตรวจติดตาม การทบทวนโดยฝ่ายบริหาร และการดำเนินการแก้ไข/ป้องกัน								
9	การตรวจรับรองระบบตามมาตรฐาน ISO 27001								

สีเขียว หมายถึง แผนระยะเวลาการปฏิบัติงานที่คาดการณ์ไว้

สีเหลือง หมายถึง ระยะเวลาการปฏิบัติจริง

จากตารางระยะเวลาการปฏิบัติ จะเห็นว่าได้แบ่งเป็นหัวข้อละ 2 แถว เป็นการแสดงการเปรียบเทียบระหว่าง การวางแผนในการปฏิบัติงาน กับการปฏิบัติงานจริง ซึ่งในการปฏิบัติงานจริงอาจไม่เป็นไปตามแผนการปฏิบัติงานที่วางไว้ โดยจะช้ากว่าแผนการที่วางไว้ในบางครั้ง และได้มาเข้าร่วมโครงงานกับพนักงานที่ปรึกษาในเดือนที่ 2 แต่เมื่อปฏิบัติงานจริง การทำทะเบียนทรัพย์สินและการประเมินความเสี่ยง จะต้องใช้เวลามากเพราะโปรแกรม อุปกรณ์ ภายในศูนย์คอมพิวเตอร์มีจำนวนมาก การประเมินความเสี่ยงและแก้ไขความเสี่ยงจึงต้องใช้เวลามากพอสมควร หลังจากสองส่วนนี้ก็ปฏิบัติได้ตามกำหนด

3.2 รายละเอียดงานที่ได้รับมอบหมาย

1) จัดทำกระบวนการบริหารความเสี่ยง (Risk Management) จัดทำแผนปฏิบัติการเพื่อลดความเสี่ยง (Risk Treatment Plan) ภายในศูนย์คอมพิวเตอร์ (Data Center) เพื่อใช้ในการประเมินความเสี่ยง

2) ช่วยพนักงานที่ปรึกษาวิเคราะห์ความเสี่ยงเพื่อหามาตรการป้องกันศูนย์คอมพิวเตอร์ (Data Center) ให้มีความเสี่ยงที่ลดน้อยลง และมีความครอบคลุมตามมาตรฐาน ISO 27001

3) ช่วยปรับปรุงห้อง ศูนย์คอมพิวเตอร์ (Data Center) ให้ตรงกับข้อกำหนดเพื่อรักษาความปลอดภัย

4) การจัดทำ Policy ในศูนย์คอมพิวเตอร์

3.3 ขั้นตอนการดำเนินงาน

3.3.1 จัดตั้งคณะทำงาน IT Security Steering หรือ IT Security Working Group

ทำเรื่องมาตรฐาน ISO/IEC 27001 และ Regulatory Compliance เพื่อทำการศึกษาตัวมาตรฐานโดยละเอียดและหาแนวทางนำมาปรับประยุกต์ใช้ภายในองค์กร

3.3.2 จัดฝึกอบรม

ทำความเข้าใจในส่วนของข้อกำหนดทั้ง 11 โดเมน ของมาตรฐานISO/IEC 27001 โดยการฝึกอบรมโดยใช้แนวทางในการทำ Internal ISO 27001 Workshop ซึ่งทำให้ทีมงานได้เข้าใจแนวทางของการตรวจสอบโดยการนำมาตรฐานISO/IEC 27001 มาใช้อย่างถูกต้องเหมาะสำหรับ

องค์กรที่ต้องการได้รับใบรับรองจากผู้ให้บริการออกใบรับรอง หรือ Certification Body เพื่อเป็นการเตรียมตัวในการตรวจสอบเพื่อผ่านการรับรองต่อไป ในส่วนขององค์กรที่ผู้บริหารระดับสูงมีแนวคิดเรื่องการปรับปรุงระบบการรักษาความมั่นคงปลอดภัยภายในองค์กรแต่ไม่จำเป็นต้องได้รับการรับรองจาก Certification Body ก็ควรศึกษามาตรฐานสากลจากตัวต้นฉบับที่เป็นภาษาอังกฤษ และ ศึกษาแนวทางในการปฏิบัติจากมาตรฐาน ISO/IEC 27002 เพื่อที่จะได้รายละเอียดในการประยุกต์ใช้เพิ่มมากยิ่งขึ้น เพราในส่วนของมาตรฐาน ISO/IEC 27001 นั้นเน้นไปที่ Checklist หรือ Requirement ที่ทาง ISMS Auditor ใช้ในการตรวจสอบระบบ แต่ไม่ได้มีคำอธิบายแนวทางปฏิบัติ หรือ Guideline ไว้ในตัวมาตรฐาน แต่มาตรฐาน ISO/IEC 27002 นั้นจะเน้นไปที่ Code Of Practices ที่สามารถนำมาอ้างถึงเป็นแนวทางในการปฏิบัติ รวมทั้งมีการยกตัวอย่างประกอบความเข้าใจ ทำให้ผู้ที่ต้องการนำมาตรฐานมาประยุกต์ใช้เกิดความเข้าใจมากยิ่งขึ้น

3.3.3 จัดทำการประเมินระบบในภาพรวม (Holistic Approach)

โดยนำเทคนิค “Gap Analysis” มาใช้ กล่าวคือ นำมาตรฐาน ISO/IEC 27001 ในส่วน Control ที่อยู่ใน Annex A. มาทำเป็นประโยคคำถามในรูปแบบของ Questionnaire มาใช้ในการสัมภาษณ์ผู้ที่เกี่ยวข้องในองค์กรในลักษณะ Workshop ที่ทุกคนสามารถเข้ามามีส่วนร่วมในการตอบคำถามและให้ความเห็น รายงานจากการทำ Gap Analysis จะทำให้ผู้บริหารระดับสูงขององค์กรได้ทราบถึงสถานะล่าสุดขององค์กร (ASIS) และ ความแตกต่างกับข้อกำหนดในมาตรฐาน ว่าระบบในองค์กรยังไม่ได้ปฏิบัติตามข้อกำหนดในมาตรฐานและมีความแตกต่างจาก “สิ่งที่ควรจะเป็น” หรือ “สิ่งที่ควรจะต้องทำ” ตามมาตรฐานอย่างไร

3.3.4 หลังจากการทำ “Gap Analysis Workshop”

แล้วควรมีการจัดทำรายงานและมีการนำเสนอต่อ Board of Director เพื่อที่จะให้ผู้บริหารระดับสูงเกิดความเข้าใจในปัญหาที่เกิดขึ้น และ สร้าง “Management Buy-In” คือ การทำให้ผู้บริหารระดับสูงตัดสินใจให้การสนับสนุนในการปฏิบัติตามมาตรฐาน ISO/IEC 27001 และดำเนินการแก้ไขข้อบกพร่องจากการที่องค์กรยังไม่ได้ปฏิบัติตามมาตรฐานดังกล่าวอย่างเป็นรูปธรรม (Corrective Action)

3.3.5 ทำรายละเอียดหลังจากการนำเสนอ Gap Analysis Report

โดยการทำกระบวนการบริหารความเสี่ยง (Risk Management) ในสามมุมมอง ได้แก่ มุมมองด้านบุคลากร (People) มุมมองด้านกระบวนการ (Process) และ มุมมองด้านเทคโนโลยี (Technology) เพื่อที่จะได้ประเมินความเสี่ยง (Risk Assessment) ของระบบ และ จัดทำแผนปฏิบัติการเพื่อลดความเสี่ยง (Risk Treatment Plan) เช่น การทำ Hardening การจัดฝึกอบรม Security Awareness Training ในองค์กร การจัดทำระบบ Centralized Log Management เพื่อปฏิบัติตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 และ เป็นการปฏิบัติตามพรบ.การกระทำผิดเกี่ยวกับคอมพิวเตอร์

3.3.6 ทำ Implement

ปฏิบัติตามแผนที่ได้กำหนดไว้จากขั้นตอนที่ 5 เช่นการทำ Vulnerability Assessment หรือ Penetration Testing การปิดช่องโหว่ด้วยการ Hardening หรือ การติดตั้ง Patch ให้กับระบบ การจัดทำ Policy, Standard, Guideline ต่าง ๆ ที่จำเป็น การฝึกอบรม Security Awareness Program ให้กับทุกคนในองค์กร การจัดทำ Acceptable Use Policy (AUP) การจัดซื้อจัดจ้างฮาร์ดแวร์และซอฟต์แวร์ในส่วนของเทคโนโลยีที่จำเป็น เช่น Firewall, Anti-Virus Software เป็นต้น

3.3.7 การติดตามผล

ควรมีการตรวจผล (Review) และ การเฝ้าระวัง (Monitor) เพื่อเปรียบเทียบความเปลี่ยนแปลงระหว่างก่อนการปฏิบัติตามมาตรฐาน และ หลังจากการปฏิบัติตามมาตรฐาน (Before and After) ก็จะเห็นผลลัพธ์ในเชิงบวกที่เป็นรูปธรรมชัดเจน และ ควรทำการเฝ้าระวังระบบด้วยแนวคิด “Continuous Audit” เพื่อที่จะได้แน่ใจว่าระบบสามารถทำงานได้ปกติโดยไม่เกิดผลกระทบจากการค้นพบช่องโหว่ใหม่ ๆ (New Vulnerability) และ ภัยใหม่ ๆ จาก Hacker หรือ Malicious Software ต่าง ๆ (New Threat) ตลอดจนสามารถปรับตัวแก้ไขปัญหาได้อย่างทันท่วงที (Agility)

ในขั้นตอนสุดท้ายนี้ การ Outsource ไปยัง Manage Security Service Provider หรือ MSSP ถือเป็นการ “Transfer Risk” ที่ผู้บริหารควรนำมาเป็นทางเลือกอีกทางหนึ่งในการลดความเสี่ยงให้แก่องค์กร โดยความรับผิดชอบในส่วนนี้ทาง MSSP จะต้องเป็นผู้รับผิดชอบ โดยกำหนดไว้ใน Services Level Agreement (SLA) ให้ชัดเจน

จาก 7 ขั้นตอนดังกล่าว ทีมงานจะสามารถจัดทำเอกสารในรูปแบบ Statement of Applicability (SOA) เพื่อจัดเตรียมให้ทางผู้ตรวจสอบตามกระบวนการ ISMS (ISMS Auditor หรือ ISMS Lead Auditor) จากหน่วยงานที่ให้บริการออกใบรับรอง (Certification

Body) เข้ามาตรวจสอบ เพื่อนำไปสู่ขั้นตอนการ “Certify” มาตรฐาน ISO/IEC 27001 ต่อไปในอนาคต ซึ่งสามารถนำไปต่อยอดได้ทั้ง 7 ขั้นตอน และ ยังทำให้ภาพลักษณ์ขององค์กรต่อสาธารณะชน ตลอดจนลูกค้าและคู่ค้าเกิดความมั่นใจในการรักษาความมั่นคงปลอดภัยระบบขององค์กรที่ได้ตามมาตรฐานสากลอีกด้วย นอกจากประโยชน์ในด้านความปลอดภัยระบบที่เพิ่มขึ้นและเพื่อความยั่งยืนขององค์กรต่อไปในอนาคต

บทที่ 4 สรุปผลการดำเนินงาน การวิเคราะห์และสรุปผลต่าง ๆ

4.1 สรุปผลการดำเนินงาน

ในการปฏิบัติงานสหกิจศึกษา ณ สถานที่ประกอบการเป็นเวลา 4 เดือน ได้มีการดำเนินงานของโครงการนี้แบ่งเป็นระยะ การดำเนินงานได้ดังต่อไปนี้

1) ทำความเข้าใจในส่วนของข้อกำหนดทั้ง 11 โดเมน ของมาตรฐานISO/IEC 27001 โดยการฝึกอบรมโดยใช้แนวทางในการทำ Internal ISO 27001 Workshop

2) ทำกระบวนการบริหารความเสี่ยง (Risk Management) ใน 3 มุมมอง ได้แก่ มุมมองด้านบุคลากร (People) มุมมองด้านกระบวนการ (Process) และ มุมมองด้านเทคโนโลยีสารสนเทศ (Technology) แล้วนำมาประเมินความเสี่ยง

3) พัฒนานโยบายทางด้านสารสนเทศโดยการนำมาตรฐาน ISO27001มาประยุกต์ใช้แล้วจัดทำนโยบายด้านสารสนเทศขององค์กร

4.2 การวิเคราะห์และสรุปผลต่าง ๆ

จากการได้ทำการศึกษา และลงมือปฏิบัติ ตามงานที่ได้รับมอบหมายมาให้ในแต่ละส่วนสรุปผลได้ดังต่อไปนี้

4.2.1 Security Policy

1) ปรับปรุงนโยบายให้คลอบคุลมหัวข้อการรักษาความมั่นคงปลอดภัยตามข้อกำหนดของมาตรฐาน ISO 27001 เช่น การบริหารความเสี่ยงด้านความมั่นคงปลอดภัย การบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัย การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ เป็นต้น รวมถึงจัดทำนโยบายหัวข้ออื่น ๆ ตามความเหมาะสม

2) ได้มีการกำหนดระยะเวลาในการทบทวนและปรังปรุงนโยบายให้ทันสมัยและทำการทบทวน ปรับปรุงนโยบายตามรอบระยะเวลาดังกล่าวหรือเมื่อมีความเปลี่ยนแปลงที่สำคัญเกิดขึ้น

4.2.2 Organization of Information Security

1) กำหนดหน่วยงานเฉพาะด้านความมั่นคงปลอดภัยของข้อมูล คณะทำงาน หรือตัวแทนที่เหมาะสมจากส่วนงานที่เกี่ยวข้องเพื่อร่วมพิจารณาในประเด็นด้านความมั่นคงปลอดภัยของข้อมูล เช่น การบริหารความเสี่ยง การจัดการเหตุละเมิดความมั่นคงปลอดภัย

2) กำหนดนโยบาย สร้างกระบวนการเพื่อควบคุม และอนุมัติการนำอุปกรณ์ใหม่ อุปกรณ์ส่วนตัว หรือระบบจัดหาซื้อเพิ่ม มาใช้งานภายในองค์กร

3) จัดให้บุคคลภายนอกหรือหน่วงงานภายนอกเช่น ผู้ให้บริการ (Vendor) หรือ ผู้เชี่ยวชาญจากภายนอกที่สามารถเข้าถึงข้อมูลสำคัญขององค์กรได้มีการลงนามข้อตกลงในการรักษาความลับ

4) รวบรวมรายชื่อและเบอร์ติต่อของหน่วงงานที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัย และกำหนดขึ้นตอนที่ชัดเจนในการติดต่อประสานงานเมื่อเกิดเหตุละเมิดความมั่นคงปลอดภัยขึ้น

5) ทบทวนความถูกต้องของรายชื่อและเบอร์ติดต่อของหน่วยงานที่เกี่ยวข้องอย่างสม่ำเสมอ

6) จัดให้มีกระบวนการที่ชัดเจนในการรับข่าวสาร การแลกเปลี่ยนข้อมูล และการติดต่อประสานงานกับหน่วงงานหรือผู้เชี่ยวชาญ เมื่อเกิดเหตุละเมิดความมั่นคงปลอดภัยขึ้น

7) จัดทำกระบวนการระบุและประเมินความเสี่ยงจากหน่วงงานภายนอกที่จำเป็นต้องเข้าถึงระบบสารสนเทศ ข้อมูล และดำเนินการแก้ไขความเสี่ยงด้วยวิธีการที่เหมาะสม

8) กำหนดระเบียบควบคุมการร้องขอเข้าถึงพื้นที่ การขอติดตั้งเคลื่อนย้าย และการขอใช้บริการของศูนย์คอมพิวเตอร์ (Data Center)

9) จัดให้มีกระบวนการในการกำหนดข้อตกลง และหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลสำหรับหน่วงงานภายนอก โดยพิจารณาตามเสี่ยงที่เกี่ยงข้องกับหน่วยงานนั้น ๆ

4.2.3 Asset Management

1) จัดทำทะเบียนทรัพย์สิน ให้ครอบคลุมทรัพย์สินทุกประเภทตามข้อกำหนดของมาตรฐาน ISO 27001

2) จัดทำนโยบายการใช้งานข้อมูลและทรัพย์สินสารสนเทศอย่างเหมาะสม โดยครอบคลุมข้อมูล และทรัพย์สินที่เกี่ยวข้องในการประมวลผลข้อมูล และบังคับใช้กับทุกคนที่เป็นผู้ใช้งานทั้งที่เป็นพนักงานและบุคคลภายนอก

3) จัดทำนโยบายในการแบ่งระดับชั้นความลับของข้อมูล โดยพิจารณาจากความสำคัญของข้อมูล ความต้องการทางกฎหมายให้เหมาะสมกับองค์กร

4) กำหนดวิธีการใช้งานข้อมูลที่เหมาะสมตามระดับชั้นความลับที่กำหนดไว้โดยคลอบคลุมตั้งแต่ การระบุชั้นความลับของข้อมูล การจัดเก็บ การรับ-ส่ง การใช้งานและการทำลาย ที่สอดคล้องกับระเบียบว่าด้วยการรักษาความลับของทางราชการ

4.2.4 Human resources security

1) กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยให้กับพนักงานแต่ละตำแหน่ง คู่สัญญาและผู้ให้บริการภายนอกโดยพิจารณาจากหน้าที่งาน นโยบายและขั้นตอนการปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูล

2) จัดอบรม หรือจัดทำคู่มือการปฏิบัติสำหรับผู้ให้บริการภายนอก เพื่อให้สามารถปฏิบัติตามระเบียบ นโยบาย และขั้นตอนปฏิบัติขององค์กรได้อย่างถูกต้อง

3) จัดทำแผนการอบรมเพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของหน่วยงานให้กับพนักงานทุกคน รวมถึงผู้ให้บริการภายนอกที่เข้ามาปฏิบัติหน้าที่ภายในหน่วยงาน และจัดเก็บบันทึกการฝึกอบรม

4) เพิ่มเติมเนื้อหาในสัญญาจ้างที่ระบุถึงหน้าที่ความรับผิดชอบที่ต้องปฏิบัติภายหลังสิ้นสุดการจ้างงาน โดยเฉพาะตำแหน่งงานสำคัญ และผู้ให้บริการภายนอกที่รับทราบข้อมูล หรือปฏิบัติงานสำคัญ พร้อมทั้งแจ้งให้พนักงาน และผู้ให้บริการภายนอกรับทราบถึงหน้าที่ความรับผิดชอบเมื่อสิ้นสุดสัญญาจ้าง

5) จัดทำบัญชีควบคุมการถือครองทรัพย์สินองค์กรของพนักงาน และจัดให้มีกระบวนการในการตรวจสอบและเรียกคืนทรัพย์สินเมื่อพนักงานลาออกหรือโยกย้ายตำแหน่งงานอย่างครบถ้วน

6) จัดทำขั้นตอนปฏิบัติงานสำหรับการถอดถอนสิทธิเมื่อพ้นสภาพ หรือโยกย้าย

4.2.5 Physical and environmental security

1) พิจารณาปรับปรุงโครงสร้างของศูนย์คอมพิวเตอร์ให้มั่นคงแข็งแรง และพิจารณาใช้วัสดุที่ไม่ติดไฟ หรือวัสดุทนไฟในการก่อสร้าง และติดตั้งระบบตรวจสอบต่าง ๆ ที่สำคัญ เช่น ระบบตรวจจับน้ำรั่ว เป็นต้น

2) รายละเอียดของบุคคลภายนอกไว้ให้เพียงพอแก่การใช้อ้างอิง และติดตามหากจำเป็น

3) ติดตั้งระบบ CCTV เพื่อเฝ้าติดตามดูผู้ให้บริการภายนอกที่เข้ามาปฏิบัติงานในพื้นที่ตลอดเวลา รวมถึงการเข้าออกพื้นที่ควบคุม

4) จัดทำระเบียบการเข้าปฏิบัติงานในศูนย์คอมพิวเตอร์ให้ครอบคลุมประเด็นด้าน

5) ความมั่นคงปลอดภัย

6) กำหนดวิธีการตรวจสอบพัสดุและสินค้า เพื่อค้นหาสิ่งแปลกปลอมที่อาจเป็นอันตรายก่อนขนย้ายเข้าพื้นที่ชั้นใน

7) กำหนดให้มีการล็อคตู้ Rack ทุกครั้ง

8) ปรับปรุงพื้นที่วางอุปกรณ์สารสนเทศของฝ่ายให้แยกออกจากพื้นที่ของหน่วยงานอื่น และควบคุมสิทธิการเข้าถึง

9) จัดระเบียบสายไฟและสายสัญญาณ โดยเดินสายร้อยท่อหรือใช้ทางเดินสายอย่างเหมาะสม

10) กำหนดวิธีการที่เป็นมาตรฐานสำหรับทำป้ายฉลาก (Label) และดำเนินการติดป้ายฉลากให้แก่สายสัญญาณและสายไฟให้ครบถ้วน

11) จัดทำแผนผังการเชื่อมต่อสายสัญญาณและสายไฟให้ครบถ้วน

12) กำหนดนโยบายควบคุมการใช้งานอุปกรณ์นอกพื้นที่ โดยระบุว่าอุปกรณ์ใดได้รับอนุญาตให้นำออกไปใช้งานภายนอกได้บ้าง

13) จัดทำวิธีปฏิบัติในการนำอุปกรณ์ออกไปใช้นอกพื้นที่อย่างมั่นคงปลอดภัย จัดทำวิธีการปฏิบัติในการทำลายข้อมูลและซอฟท์แวร์ลิขสิทธิ์ในอุปกรณ์และสื่อบันทึกอย่างมั่นคงปลอดภัย

14) จัดทำขั้นตอนควบคุมการนำอุปกรณ์ออกจากพื้นที่โดยให้มีการขออนุมัติ การกำหนดระยะเวลาที่ให้นำออก และบันทึกรายละเอียดไว้สำหรับตรวจสอบการนำกลับคืน

4.2.6 Communications and operations management

1) กำหนดขั้นตอนให้มีการปรับปรุงเอกสารให้เป็นปัจจุบันเมื่อมีการเปลี่ยนแปลงเกิดขึ้นกับระบบ

2) จัดทำขั้นตอนปฏิบัติงานที่เป็นมาตรฐานกลางและให้ครอบคลุมการบริหารจัดการการเปลี่ยนแปลงตลอดกระบวนการ

3) สร้างกระบวนการในการบริหารจัดการ Capacity เพื่อให้มีการติดตามตรวจสอบปริมาณการใช้งาน ตลอดจนวิเคราะห์แนวโน้มการใช้งานและการเปลี่ยนแปลงในอนาคต

4) จัดทำนโยบายในการควบคุมการใช้งานสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ให้มีความมั่นคงปลอดภัย

5) จัดทำนโยบายและขั้นตอนปฏิบัติในการทำลายสื่อบันทึกข้อมูลในรูปแบบต่าง ๆ ด้วยวิธีการที่มั่นคงปลอดภัย

6) จัดทำนโยบายเพื่อควบคุมการถือครองข้อมูล การจัดเก็บ การรับ-ส่ง การใช้งาน

7) การเก็บรักษา และการทำลายข้อมูลแต่ละประเภทตามระดับชั้นความลับ

8) กำหนดวิธีการจัดเก็บและปกป้องเอกสารคู่มือระบบงานต่าง ๆ อย่างเหมาะสม

9) จัดทำนโยบายในการแลกเปลี่ยนข้อมูลขององค์กรกับหน่วยงานทั้งภายในและภายนอกผ่านช่องทางการสื่อสารต่าง ๆ ให้เป็นไปอย่างมั่นคงปลอดภัย

10) จัดทำนโยบายเพื่อควบคุมการขนย้ายสื่อบันทึกข้อมูลรูปแบบต่าง ๆ ให้เป็นไปอย่างมั่นคงปลอดภัย และป้องกันการรั่วไหลของข้อมูล

11) กำหนดนโยบายควบคุมการใช้โปรแกรมประเภท Instant Massaging และช่องทางการรับส่งข้อมูลทางอิเล็กทรอนิกส์อื่น ๆ

12) ทำการ Hardening Server ตามวิธีที่เหมาะสม โดยผู้ที่มีความเชี่ยวชาญเพียงพอ

13) จัดทำขั้นตอนปฏิบัติงาน และกำหนดรูปแบบ และวิธีการในการติดตามตรวจสอบ และวิเคราะห์ Log ของระบบตามความเหมาะสม

14) กำหนดให้มีการจัดเก็บ Log การปฏิบัติงานของผู้ดูแลระบบและพนักงานที่เกี่ยวข้องกับระบบ ทั้งในส่วนของ Log ที่บันทึกโดยระบบ และบันทึกโดยพนักงาน

15) ทำการจัดเก็บและบันทึกข้อผิดพลาด (Fault) ที่เกิดขึ้นเป็นประจำทุกวัน

16) ทำการวิเคราะห์หาสาเหตุของข้อผิดพลาดที่เกิดขึ้น และดำเนินการแก้ไขด้วยวิธีการที่เหมาะสม

4.2.7 Access Control

1) จัดทำนโยบายควบคุมการเข้าถึงระบบสารสนเทศ ที่ระบุถึงวิธีการร้องขอสิทธิ การควบคุมการเข้าถึง การจัดแบ่งกลุ่มผู้ใช้ โดยต้องต้องสัมพันธ์กับชั้นความลับของข้อมูลในระบบ

2) จัดทำขั้นตอนปฏิบัติงานสำหรับการลงทะเบียนผู้ใช้งาน และจัดทำบันทึกรายละเอียดการแจกจ่ายสิทธิระดับต่าง ๆ ของระบบ

3) กำหนดขั้นตอนที่ชัดเจนในการควบคุมการส่งมอบรหัสผ่านให้ผู้ใช้งาน

4) กำหนดวิธีการทบทวนสิทธิในการใช้งานระบบสารสนเทศของผู้ใช้งานอย่างสม่ำเสมอ โดยกำหนดรอบระยะเวลาในการทบทวนตามระดับของสิทธิ

5) จัดทำนโยบายเกี่ยวกับการป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล

6) จัดทำนโยบายควบคุมการใช้งานระบบเครือข่าย โดยระบุถึงบริการบนเครือข่ายที่เปิดให้ใช้ กลุ่มผู้ใช้งานที่สามารถใช้งานได้ การขอใช้งาน การควบคุมระบบเครือข่าย เป็นต้น

7) พิจารณาใช้เทคโนโลยี เช่น Smart card หรือ Token ช่วยในการยืนยันตัวตนเพื่อเชื่อมต่ออุปกรณ์กับระบบเครือข่าย

8) ทำการปิดตู้ Rack และใส่กุญแจทั้งหมด

9) กำหนดให้ใช้ SSH และ Telnet ในการเข้าปรับแต่งค่า Configuration ของอุปกรณ์

10) จัดทำ List ของ Share User และกำหนดผู้รับผิดชอบใน account นั้น ๆ

11) กำหนดขั้นตอนที่ชัดเจนในการขอปรับเปลี่ยน Firewall Rule

12)กำหนดนโยบายการควบคุมการนำ Mobile Computing Equipment ตามประเภทของอุปกรณ์ที่มี กำหนดนโยบายควบคุมการปฏิบัติงานจากภายนอกสำนักงาน

4.2.8 Information systems acquisition, development & maintenance

1) เพิ่มเติมเนื้อหาเรื่อง “ความต้องการด้านความมั่นคงปลอดภัย” ในเอกสารแบบฟอร์มที่ใช้ในการกำหนดคุณสมบัติของระบบสารสนเทศ เช่น เอกสาร ToR เพื่อให้มั่นใจว่าระบบสารสนเทศที่จัดซื้อ-จัดหา หรือพัฒนาขึ้น มีความมั่นคงปลอดภัยที่เหมาะสม

2) กำหนดนโยบายควบคุมการใช้งานการตรวจสอบข้อมูลนำเข้า การตรวจสอบข้อมูลในระหว่างการประมวลผล การควบคุมความถูกต้องของข้อมูลที่ถูกส่งต่อและการตรวจสอบข้อมูลนำออก โดยกำหนดหลักการในการพิจารณาว่าควรใช้งานการตรวจสอบข้อมูลนำเข้ารูปแบบใด กับข้อมูลหรือระบบใด

3) จัดทำนโยบายและกำหนดมาตรฐานการเข้ารหัสข้อมูลขององค์กร และจัดทำขั้นตอนปฏิบัติที่เกี่ยวข้อง โดยพิจารณาใช้งานเทคโนโลยีที่เหมาะสม

4) จัดทำขั้นตอนปฏิบัติควบคุมการบริหารจัดการกุญแจที่ใช้เข้ารหัสข้อมูล ตั้งแต่การสร้าง การแจกจ่าย การเปลี่ยนแปลง และการทำลายกุญแจ

5) จัดให้มีกระบวนการในการควบคุมการติดตั้งและปรับปรุงซอฟท์แวร์ได้

6) จัดให้มีมาตรการในการควบคุมข้อมูลที่นำมาใช้ในการทดสอบ

7) จัดให้มีกระบวนการในการตรวจสอบการทำงานของโปรแกรมประยุกต์ภายหลังจากที่ทำการเปลี่ยนแปลงระบบปฏิบัติการ

8) กำหนดให้มีมาตรการการควบคุม และจัดการช่องโหว่ทางเทคนิคของระบบสารสนเทศ กำหนดหน้าที่ความรับผิดชอบ และจัดหาเครื่องมือที่เหมาะสม

4.2.9 Information security incident management

1) จัดทำขั้นตอนปฏิบัติงานในการรายงานเหตุละเมิด จุดอ่อนทางด้านความมั่นคงปลอดภัย โดยกำหนดลักษณะของเหตุละเมิดที่ต้องรายงาน และ ช่องทางการรายงานที่ชัดเจน

2) จัดทำขั้นตอนปฏิบัติงานสำหรับการควบคุม และแก้ไขเหตุละเมิดความมั่นคงปลอดภัย รวมถึงกำหนดหน้าที่รับผิดชอบที่ชัดเจนสำหรับผู้ที่มีส่วนร่วมในการรับมือกับเหตุละเมิด

3) กำหนดวิธีการศึกษา วิเคราะห์ และประเมินความเสียหายของเหตุละเมิดความมั่นคงปลอดภัยที่เกิดขึ้น และดำเนินการปรับปรุงการควบคุมความเสียหายจากเหตุละเมิด

4) จัดทำแนวปฏิบัติในการเก็บหลักฐานที่เกี่ยวข้องกับเหตุละเมิดความมั่นคงปลอดภัย

5) กำหนดสิทธิการเข้าถึงข้อมูล Incident ให้เข้าได้เฉพาะผู้ที่เกี่ยวข้อง

4.2.10 Business continuity management

1) กำหนดแนวทางสำหรับการบริหารความต่อเนื่องในการดำเนินธุรกิจ ที่คลอบคลุมประเด็นด้านความมั่นคงปลอดภัยของข้อมูล

2) กำหนดวิธีการประเมินความเสี่ยงที่มีผลทำให้ธุรกิจหยุดชะงัก รวมถึงอาจดำเนินการวิเคราะห์ผลกระทบทางธุรกิจของศูนย์คอมพิวเตอร์ (Data Center) เพื่อจัดทำแผนบริหารความต่อเนื่องในการดำเนินธุรกิจและแผนสำรองฉุกเฉินด้านเทคโนโลยีสารสนเทศ

4.2.11 Compliance

1) กำหนดวิธีปฏิบัติในการระบุข้อกฎหมายที่เกี่ยวข้อง รวมถึงกำหนอแนวทางในการปฏิบัติตามกฎหมายเหล่านั้น และปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอ

2) จัดทำข้อปฏิบัติในการเก็บและควบคุมบันทึกองค์กร

3) กำหนดนโยบายในการใช้งานข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่าข้อมูลดังกล่าวจะได้รับการควบคุมอย่างเหมาะสม

4) กำหนดหน้าที่รับผิดชอบให้พนักงานระดับหัวหน้าให้มีหน้าที่ในการตรวจสอบพนักงานในเรื่องการปฏิบัติงานตามระเบียบ หรือนโยบายองค์กร

Security Domain of ISO 27001:2005	ระดับความสอดคล้อง
A.5 Information security policy	25.00%
A.6 Organization of information security	45.45%
A.7 Asset management	30.00%
A.8 Human resources security	77.78%
A.9 Physical and environmental security	34.62%
A.10 Communications and operations management	54.69%
A.11 Access control	40.00%
A.12 Information systems acquisition, development and maintenance	37.50%
A.13 Information security incident management	40.00%
A.14 Business continuity management	30.00%
A.15 Compliance	35.00%
Overall	40.91%

รูปที่ 4.1 ผลการวิเคราะห์และสรุปผลต่าง ๆ

บทที่ 5 บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

หลังจากทำโครงการนี้ พบว่าจากการวิเคราะห์ความเสี่ยง ทำให้ผู้ใช้งานในองค์กรได้ตระหนักถึงความเสี่ยงที่เกี่ยวข้องกับ ระบบสารสนเทศมากขึ้น และนำมาเป็นแนวทางในการปฏิบัติงาน ทำให้เรื่องความเสี่ยงใน ศูนย์คอมพิวเตอร์ (Data Center) ลดลงและเพิ่มประสิทธิภาพในการทำงานต่อไปในอนาคต

5.2 สรุปผลการปฏิบัติงาน

จากที่ได้ทำการประเมินความเสี่ยงที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศขององค์กรทำให้ทราบว่าระบบเทคโนโลยีสารสนเทศ ยังมีช่องโหว่อยู่และทางทีมงานได้กำลังดำเนินการลดความเสี่ยงเหล่านั้นด้วยการปิดช่องโหว่และเลือกใช้ฟังก์ชั่นของอุปกรณ์ที่มีอยู่ในการแก้ปัญหาและทำการวิเคราะห์ระบบเครือข่ายภายในองค์กรใหม่เพื่อลดความเสี่ยงที่เกิดขึ้น

5.3 ปัญหาและอุปสรรค

1) ในตอนแรก ผู้จัดทำไม่มีความรู้เกี่ยวกับการทำ ISO 27001 มาก่อน

2) เอกสารที่ได้รับมาให้ศึกษาเกี่ยวกับ ISO 27001 นั้นเป็นภาษาอังกฤษ ซึ่งบางคำเป็นคำศัพท์เฉพาะ ทำให้อ่านไม่ได้ใจความเท่าที่ควร

3) การทำทะเบียนทรัพย์สิน (Inventory Asset) ทำได้ยาก เพราะไม่เข้าใจอักษรย่อของแต่ละอุปกรณ์ จึงทำให้กรอกข้อมูลผิดประเภท

4) การเข้าร่วมประเมินความเสี่ยงในตอนแรก ผู้จัดทำไม่สามารถเข้าร่วมประเมินได้ เพราะไม่เข้าในระบบใน ศูนย์คอมพิวเตอร์ (Data Center)

5) ในการจัดประชุมแต่ละครั้งหาเวลาที่ว่างพร้อมกันได้ลำบาก

6) ข้อมูลที่เกี่ยวข้องในงานด้านนี้มีการเปิดเผยไม่มากนัก

5.4 แนวทางแก้ไข

1) เอกสารเกี่ยวกับ ISO 27001 คำศัพท์ตรงที่อ่านไม่เข้าใจถามพนักงานที่ปรึกษา

2) พนักงานที่ปรึกษาให้เข้าอบรมเพื่อศึกษามาตรฐาน ISO 27001

3) ศึกษาระบบ เพื่อสามารถเข้าร่วมในการวิเคราะห์และแก้ไขความเสี่ยงได้

4) ปรึกษากับพนักงานที่ปรึกษาในการทำโครงงาน

5.5 แนวทางในการพัฒนาต่อ

1) ทำการปรับปรุงนโยบายสารสนเทศให้ครอบคลุมมากที่สุด

2) จัดทำคู่มือขั้นตอนการปฏิบัติงานของนโยบายที่ชัดเจน ตามหัวข้อต่าง ๆ

3) ทำการแก้ไขและป้องกันความเสี่ยงในครอบคลุมทั้งหมด

4) ทำการถ่ายทอดความรู้เกี่ยวกับความปลอดภัยให้กับบุคลากรเพื่อให้บุคลากรมีความตระหนักเกี่ยวกับความปลอดภัย ตัวอย่างเช่น อบรมวิธีการป้องกันเบื้องต้น การตรวจเช็คสำหรับผู้ใช้งาน เป็นต้น

5.6 ข้อเสนอแนะ

จากการดำเนินงานและผลการดำเนินงานที่ได้นำเสนอไปนั้น ผู้จัดทำโครงการขอสรุปว่าแนวทางการพัฒนานโยบายที่ได้นำเสนอเป็นแนวทางที่ปฏิบัติตามได้ โดยต้องอาศัยศักยภาพ ของผู้พัฒนานโยบายในการทำความรู้ความเข้าใจกับข้อกำหนดต่าง ๆ จากมาตรฐานที่เลือกใช้ ถึงแม้ว่าข้อกำหนดในมาตรฐานจะมีอยู่เป็นจำนวนมาก ผู้พัฒนานโยบายต้องสามารถเลือกได้ว่า ข้อกำหนดใดส่งผลกระทบต่อความปลอดภัยของข้อมูลเป็นลำดับเริ่มต้นผู้พัฒนาไม่ได้ทำงานเพียงคนเดียว แต่ต้องอาศัยความร่วมมือและข้อมูลที่เกี่ยวข้องจากผู้ที่ได้รับผลกระทบในการพัฒนานโยบายจะต้องคำนึงถึงความรู้ความเข้าใจของผู้อ่านว่าสามารถรับรู้และปฏิบัติตามได้มากน้อยเพียงใด การพัฒนานโยบายไม่ใช้เพียงแค่การกำหนดความต้องการต่าง ๆ ตามมาตรฐานที่เลือกใช้ แต่ต้องอาศัยข้อมูลพื้นฐานจากโครงสร้างหรือการดำเนินงานขององค์กรที่เป็นอยู่ในปัจจุบันมาเป็นพื้นฐานในการพัฒนานโยบายด้วย หลังจากการพัฒนาเสร็จสิ้นและได้นำไปประกาศใช้จริงแล้ว ผู้พัฒนาควรกลับมาทบทวนและประเมินผลของการใช้งานเพื่อใช้เป็นข้อมูลในการปรับปรุงนโยบายในลำดับต่อไป

เอกสารอ้างอิง

คณะอนุกรรมการด้านความมั่นคง ภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, **ร่างแนวทางปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO27001**, 27 เมษายน 2552,

ดร. บรรจง หะรังษี, "Risk Management based on BS 7799-3:2006" ,ใน **เอกสารประกอบการสอนวิชาเลือกหัวข้อเฉพาะทางวิศวกรรมเครือข่าย1 (Audit)** ,

ยุทธพงศ์ อมรฟ้า, **มาตรฐานความปลอดภัย ISO 27001** [Online], Available: http://itm0151.blogspot.com/2009/07/iso27001.html [2011, September 8],

สุชาดา เกื้อนุ่น, **Organization Information Security Management Policy Base On ISO27001 Standard Case study for Teeya Master System Co., Ltd.**, สารนิพนธ์,

Admin, **ความปลอดภัยของข้อมูล ISO 27001 เป็นแบบไหนกันเนี่ย!!** [Online], Available: http://www.thaiblogonline.com/ittips.blog?PostID=20500 [2011, September 13],

Admin, **Risk Management : The key process for ISO 27001 implementation** [Online], Available: http://www.oknation.net/blog/print.php?id=404278 [2011, September 7],

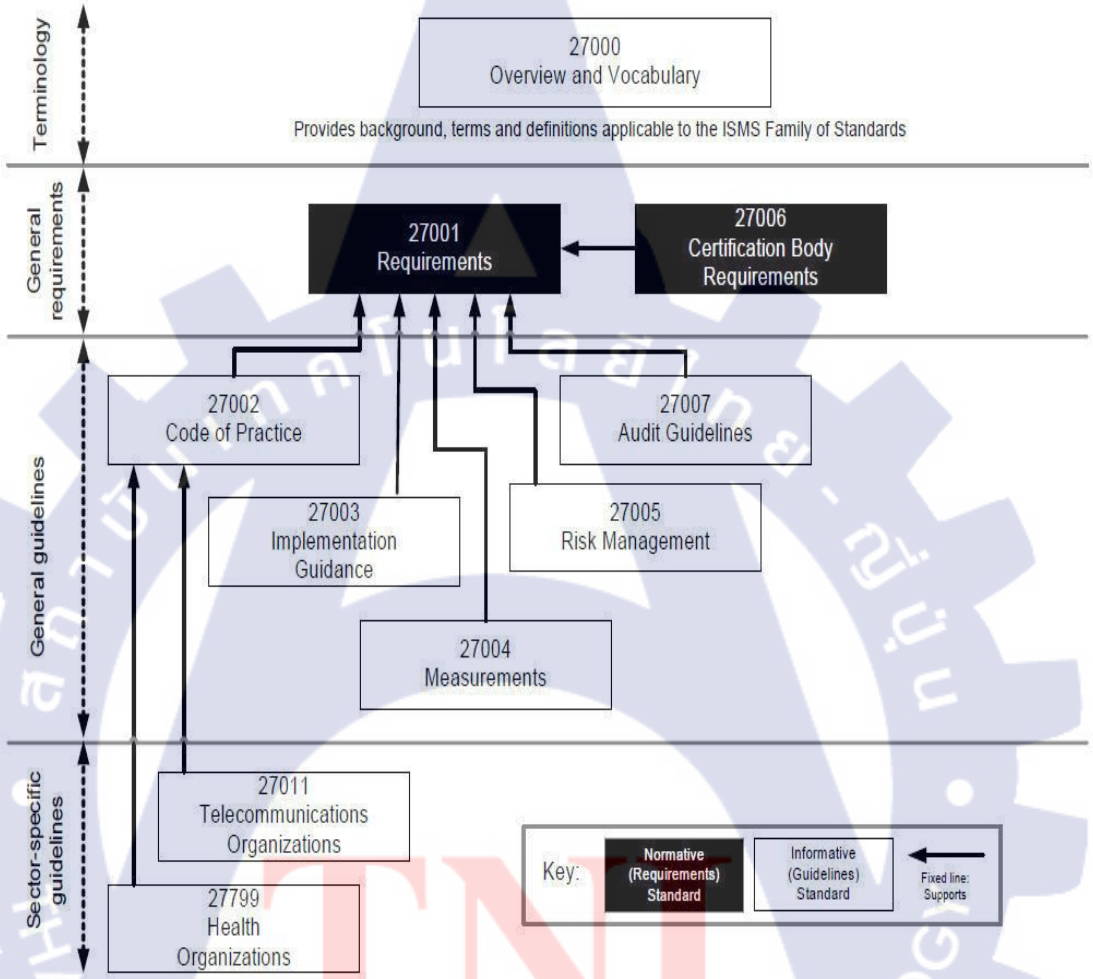
Buglive, **มาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ** [Online], Available: http://buglive.multiply.com/journal/item/7/7 [2011, September 1],

Weblog, **มาตรฐานการรักษาความมั่นคงปลอดภัย ISO/IEC 27001 และ ISO/IEC 17799 ฉบับประเทศไทย** [Online], Available: http://www.oknation.net/blog/print.php?id=404278 [2011, September 3],

ภาคผนวก

ภาคผนวก ก

ISO 27000 family standard



รูปที่ ก.1 ISO 27000 family standard

ก่อนที่จะมาเป็นมาตรฐานสากลนี้ มาตรฐาน ISO 27001 ได้ปรับปรุงมาจากมาตรฐานเดิมที่ชื่อว่า BS 7799 โดยได้พัฒนามาจาก BS7799 Part 2 : 2002 โดยถูกนำมาจัดรวมไว้ในมาตรฐานตระกูล ISO 27000 โดยมี

1) ISO 27000 Fundamentals and Vocabulary

ISO 27000 มีวัตถุประสงค์เพื่อแสดง ศัพท์และนิยาม (Vocabulary and Definitions) ที่ใช้ในมาตรฐาน นั่นคือ ศัพท์บัญญัติ (Terminology) ทั้งหลายที่ใช้ในมาตรฐานการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Standards-ISMS)

2) ISO 27001 ISMS Requirements

กำหนดมาตรฐานที่จำเป็นของ ISMS ได้แก่ คุณลักษณะเฉพาะ (Specification) ISO 27001 เป็นมาตรฐานเดียวในตระกูล ISO 27000 ที่ถูกออกแบบมาสำหรับการตรวจประเมิน(Certification) นั่นคือหากองค์กรใดได้จัดทำระบบตามมาตรฐานนี้ครบถ้วนตามความต้องการที่กำหนดไว้แล้ว องค์กรดังกล่าวสามารถยื่นคำขอไปยังหน่วยงานรับตรวจประเมินระบบ (Certification Body) เพื่อให้เข้ามาดำเนินการตรวจประเมินและรับรองระบบที่จัดทำขึ้นได้ การองค์กรหนึ่งได้รับการรับรองว่าเป็นองค์กรที่มีประสิทธิภาพการดำเนินงานในระดับมาตรฐานสากล(พัฒนามาจาก British Standard BS 7799 Part 2 ประกาศเป็น ISO/IEC ในปี 2005)

3) ISO 27002 Code of Practice

ISO 27002 จะเป็นชื่อเรียกใหม่ของ ISO 17799 ซึ่งเดิมว่า''BS 7799 Part1''เป็นมาตรฐานแสดงหลักปฏิบัติสำหรับ ISM (Code of Practice for Information Security Management) ที่อธิบายวัตถุประสงค์ของระเบียบวิธีการควบคุมด้าน IS ทั้งหลายอย่างละเอียดและแสดงรายการวิธีปฏิบัติที่ดีที่สุดของการควบคุมความมั่นคงปลอดภัย (Best Practice Security controls)

การจัดการความเสี่ยงและแผนการเตรียมพร้อมต้องคำนึงถึงความต้องการเฉพาะของแต่ละองค์กร ทั้งนี้เนื่องจากวัตถุประสงค์ในการดำเนินงานและดำเนินกิจกรรมต่าง ๆ ของแต่ละองค์กรมีความแตกต่างกัน ดังนั้นการเผชิญกับปัญหาด้านความเสี่ยงต่อภัยจากอินเทอร์เน็ต หรือไอซีทีในการประกอบธุรกรรมจึงต่างกัน ในการดำเนินโครงการ ISMS จึงต้องเริ่มต้นด้วยการประเมินความเสี่ยงขององค์กร (Risk assessment) ก่อนเสมอ โดยมีเครื่องมือคือการบริหารความเสี่ยงหรือRisk management

การบริหารความเสี่ยงเป็นการบริหารเชิงกลยุทธ์ที่สำคัญขององค์กรหมายถึงกระบวนการที่มีการดำเนินการอย่างมีระเบียบวิธีในการวิเคราะห์ความเสี่ยงที่เกี่ยวข้องกับภารกิจหรือกิจกรรมต่าง ๆ ขององค์กรเพื่อให้ภารกิจดำเนินไปได้อย่างเหมาะสม

การบริหารความเสี่ยงเป็นการชี้ระบุและบำบัดความเสี่ยงเพื่อให้ภารกิจสามารถดำเนินต่อไปได้อย่างต่อเนื่องและมีประสิทธิภาพโดยการจัดลำดับปัญหาต่าง ๆ ที่สามารถหรืออาจส่งผล

ต่อองค์กรการบริหารความเสี่ยงที่เหมาะสมทำให้เกิดโอกาสสำเร็จสูงสุดในการดำเนินภารกิจและลดโอกาสของความล้มเหลวหรือความไม่แน่นอนที่อาจมีขึ้นซึ่งการบริหารความเสี่ยงควรเป็นกระบวนการที่มีการดำเนินการและมีการพัฒนาอยู่ตลอดเวลา เพราะเงื่อนไขปัจจัยภายนอกอาจเปลี่ยนแปลงตลอดเวลา

ตัวอย่างมาตรฐานการประเมินความเสี่ยงขององค์กรด้าน IS มีหลายฉบับ เช่น 17799:2005 ซึ่งกำหนดแนวทางและเครื่องมือที่จำเป็นของมาตรฐาน ซึ่งจะเป็นกระบวนการจัดการด้านความมั่นคงปลอดภัยสารสนเทศดังนี้

1) นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)

2) การจัดตั้งองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

3) การบริหารจัดการทรัพย์สิน (Asset Management)

4) ปัจจัยความปลอดภัยทางบุคลากร (Human Resource Security)

5) ปัจจัยความปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical & Environment Security)

6) การบริหารจัดการด้านการสื่อสารและการดำเนินงาน (Communications & Operation Management

7) ปัจจัยความปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical & Environment Security)

8) การบริหารจัดการด้านการสื่อสารและการดำเนินงาน (Communications & Operation Management)

9) การควบคุมการเข้าถึง (Access Control)

10)การควบคุมการเข้าถือสิทธิ์ การพัฒนาและดูแลระบบสารสนเทศ (Information Systems Acquisition, Development & Maintenance)

11)การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

12)การบริหารความต่อเนื่องของการดำเนินงาน (Business Continuity Management)

13)การปฏิบัติตามข้อกำหนดทางกฎหมายและบทลงโทษของการละเมิดนโยบายด้านความมั่นคงปลอดภัย (Compliance)

4) **ISO 27003 ISMS Implementation Guidelines** เป็นแนวทางประยุกต์ใช้มาตรฐาน (Implementation Guide)

5) **ISO 27004 ISM Measurements** จะเป็นมาตรฐานการวัด ISM เพื่อที่จะช่วยวัดประสิทธิภาพหรือประเมินผลการนำ ISMS ไปใช้

6) **ISO 27005 ISMS Risk Management**เป็นมาตรฐาน''การบริหารจัดการความเสี่ยงด้าน IS(Information Security Risk Management'' ซึ่งจะมาแทนที่มาตรฐานเดิม ได้แก่ ''BS 7799 Part3''

7) **ISO 27006 ISMS Accreditation Guidelines** เป็นแนวทางปฏิบัติสำหรับกระบวนการออกใบรับรอง (Certification process) หรือการลงทะเบียน (Registration process) ให้กับหน่วยงานที่เกี่ยวข้อง (ISMS certification registration bodies

ภาคผนวก ข

การวิเคราะห์ความเสี่ยงและการประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงโดยส่วนมากจะทำการประเมิน และให้ค่าต่าง ๆ ในเชิง Quantitative (ปริมาณ) เนื่องจาก ผลกระทบต่าง ๆ ที่อาจเกิดขึ้นต่อข้อมูลและทรัพย์สินขององค์กรนั้น อาจจะก่อให้เกิดความเสียหายในด้านของตัวเงิน ที่สามารถวัดได้ในเชิง Quantitative (ปริมาณ) ส่วนการประเมินแบบ Qualitative (คุณภาพ) เช่น ชื่อเสียงและ ภาพลักษณ์ขององค์กร การเสียโอกาสในเชิงธุรกิจ ซึ่งอาจจะประเมินค่าเป็นตัวเงินได้ลำบาก หรือไม่สามารถประเมินค่าได้ ดังนั้นโครงงานจึงเลือกวิธีการประเมินแบบ Quantitative (ปริมาณ) โดยใช้ Risk calculation

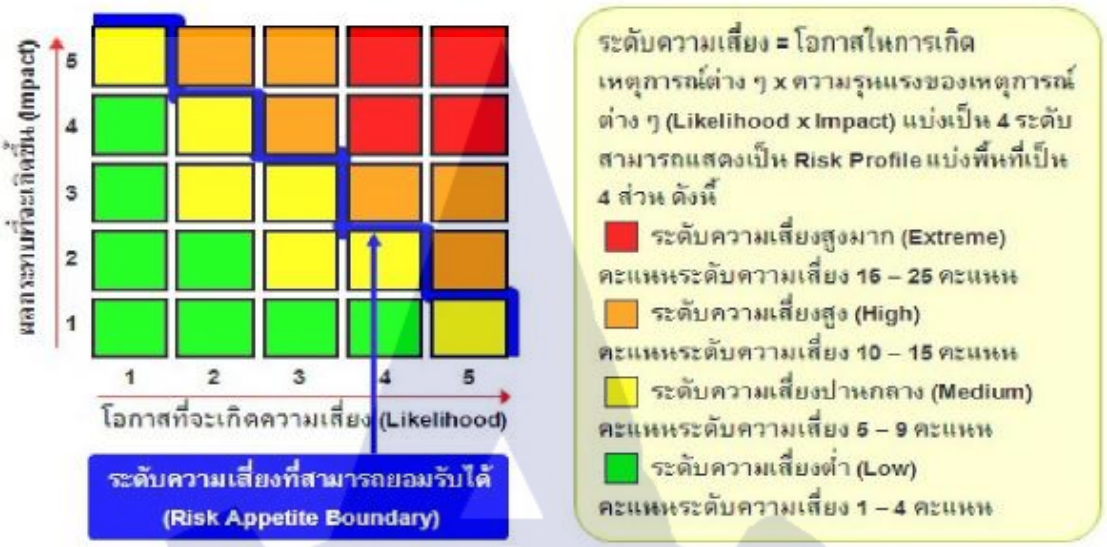
ตารางที่ ข.1 ตารางคำนวณการประเมินความเสี่ยง

	Likelihood	Very Low	Low	Middle	High	Very High
Impact	Very Low	1	2	3	4	5
	Low	2	4	6	8	10
	Middle	3	6	9	12	15
	High	4	8	12	16	20
	Very High	5	10	15	20	25

Risk Value = Likelihood * Impact

Likelihood = โอกาสที่จะเกิด

Impact = ผลกระทบ



รูปที่ ข.1 ระดับความเสี่ยง (Degree of risk)

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ (Likelihood)		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	มีโอกาสในการเกิดสูงมาก
4	สูง	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อย ๆ
3	ปานกลาง	มีโอกาสเกิดบ้างเป็นบางครั้ง
2	น้อย	อาจมีโอกาสเกิดแต่นาน ๆ ครั้ง
1	น้อยมาก	แทบไม่มีโอกาสเกิดขึ้นเลย

รูปที่ ข.2 ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ

ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact)		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุที่แก้ไขได้
1	น้อยมาก	เกิดเหตุที่ไม่มีความสำคัญ

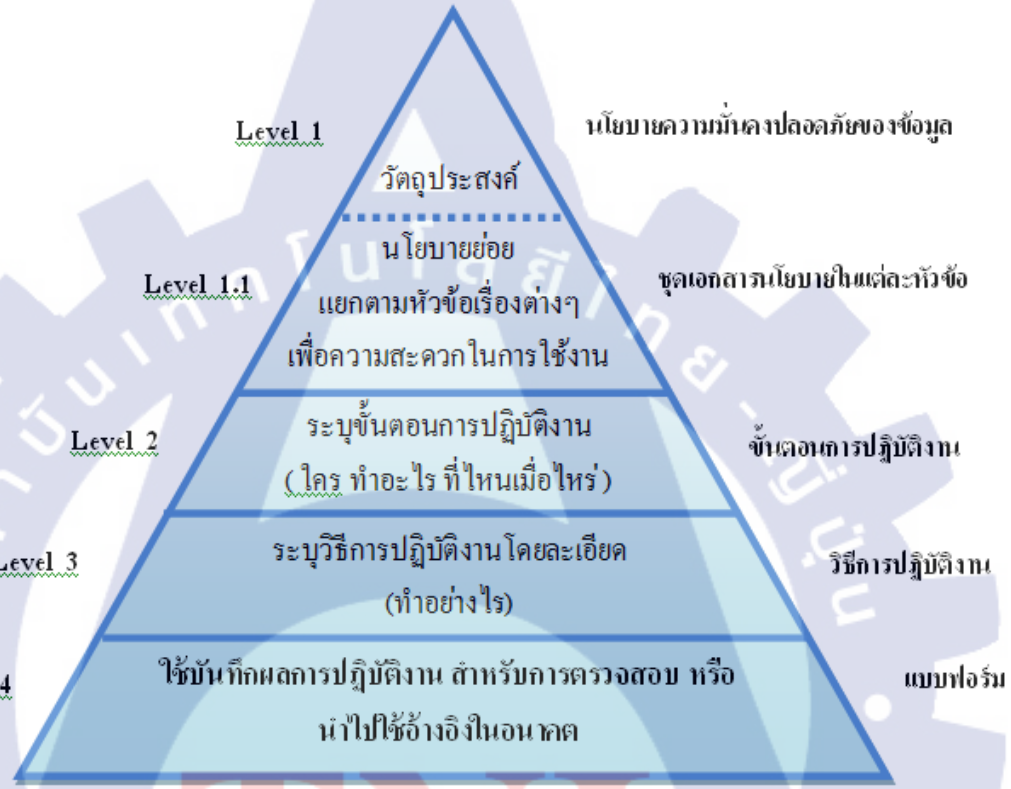
รูปที่ ข.3 ระดับความรุนแรงของผลกระทบของความเสี่ยง

ตารางที่ ข.2 ตารางการประเมินระดับความเสี่ยง

Level of Risk	Risk
1-8	Low
9-16	Medium
17-25	High

ภาคผนวก ค
การจัดทำนโยบายความมั่นคงปลอดภัยให้มีประสิทธิภาพ

โครงสร้างของเอกสารนโยบายตามแนวของมาตรฐาน ISO 27001



รูปที่ ค.1 โครงสร้างเอกสารนโยบาย

1) Level 1 นโยบาย

1.1 กำหนดวัตถุประสงค์และความต้องการด้านความมั่นคงปลอดภัยขององค์กรในระดับสูง

1.2 ไม่จำเป็นต้องปรับปรุงแก้ไขบ่อยครั้ง

1.3 เนื้อหาเป็นภาพกว้างเพื่อความยืดหยุ่น

1.4 ลงนามโดยผู้บริหารระดับสูง

1.5 ต้องการเอกสารสนับสนุนในระดับล่าง (Level 2,3,4) เพื่อให้บรรลุวัตถุประสงค์

2) Level 1.1 นโยบายย่อย

2.1 กล่าวถึงการรักษาความมั่นคงปลอดภัยในด้านใดด้านหนึ่งแบบเฉพาะเจาะจง

2.2 มีรายละเอียดมากกว่า Level 1 จึงมีโอกาสเปลี่ยนแปลงบ่อย และต้องการการทบทวนบ่อยครั้งมากกว่า

3) Level 2 ขั้นตอนการปฏิบัติงาน

3.1 ระบุ “ใคร” ที่ต้องเป็นผู้ปฏิบัติตามข้อกำหนดของนโยบาย

3.2 ระบุว่าต้องปฏิบัติ “อะไร”

3.3 การปฏิบัตินั้นต้องกระทำ “ที่ไหน”

3.4 และ การปฏิบัตินั้นต้องกระทำ “เมื่อไหร่”

3.5 ขั้นตอนการปฏิบัติงาน ช่วยให้นโยบายสามารถบังคับใช้ได้จริง

3.6 ขั้นตอนการปฏิบัติงาน กำหนดขั้นตอนที่ต้องทำตามลำดับ สำหรับงานแต่ละประเภท

3.7 สามารถใช้เป็นเอกสารอ้างอิงในการปฏิบัติงานจริงได้

3.8 ต้องได้รับการทดสอบ ทบทวน และปรับปรุงบ่อยครั้ง เพื่อให้พนังงานสามารถนำไปใช้อ้างอิงได้

ตัวอย่าง

- ขั้นตอนปฏิบัติงานในการรับมือเหตุละเมิดความมั่นคงปลอดภัย
- ขั้นตอนปฏิบัติงานในการอนุมัติและเพิกถอนสิทธิของระบบสารสนเทศ
- ขั้นตอนปฏิบัติงานในการสำรองข้อมูล

4) Level 3 วิธีการปฏิบัติงาน

4.1 ระบุวิธีปฏิบัติว่าต้องทำ “อย่างไร”

4.2 ให้รายระเอียดวิธีการทำงานสำหรับงานแต่ละประเภท

4.3 ต้องได้รับการทดสอบ ทบทวน และปรับปรุงบ่อยครั้ง เพื่อให้พนักงานสามารถนำไปใช้อ้างอิงได้

4.4 สามารถแยกย่อยได้เป็น

4.4.1 วิธีการปฏิบัติงาน (Work Instruction)

4.4.2 มาตรฐาน (Standard)

4.4.3 แนวปฏิบัติ (Guideline)

4.4.4 รายการปฏิบัติ (Checklist)

ตัวอย่าง

- วิธีการปฏิบัติงานในการลบทำลายข้อมูลแบบมั่นคงปลอดภัย
- วิธีการปฏิบัติงานในการสำรองค่าการปรับแต่งของระบบสารสนเทศ

มาตรฐาน

เป็นกฎ ระเบียบ หรือคำสั่ง ที่ออกโดยผู้มีอำนาจ ซึ่งต้องปฏิบัติตามอย่างเคร่งครัดระบุข้อมูล โดยมีคุณสมบัติ กรรมวิธี หรือรายละเอียดของผลลัพธ์ที่ต้องการและต้องการการทบทวนเพื่อให้มั่นใจว่ามีความเหมาะสม

ตัวอย่าง

- มาตรฐาน Firewall ขององค์กร
- มาตรฐานซอฟต์แวร์ขององค์กร
- มาตรฐานการเข้ารหัสขององค์กร
- มาตรฐานรหัสผ่านขององค์กร

แนวปฏิบัติ

การให้คำแนะนำที่ดี แต่อาจไม่จำเป็นต้องปฏิบัติตาม หรือปฏิบัติไม่ครบถ้วนก็ได้

รายการปฏิบัติ

ระบุสิ่งที่ต้องปฏิบัติ สำหรับงานประเภทใดประเภทหนึ่ง ต้องเขียนในลักษณะข้อความสั้นและมีการลำดับความสำคัญ เพื่อสามารถใช้เป็นเครื่องมือในการตรวจสอบหรือทบทวนได้ อาจใช้การบันทึกข้อมูลได้ (ใช้เป็นแบบฟอร์ม)

ตัวอย่าง

- รายการปฏิบัติเพื่อเปิด-ปิดระบบงานในช่วงวันหยุดยาว
- รายการปฏิบัติเพื่อการตรวจสอบภายใน

5) Level 4 แบบฟอร์ม

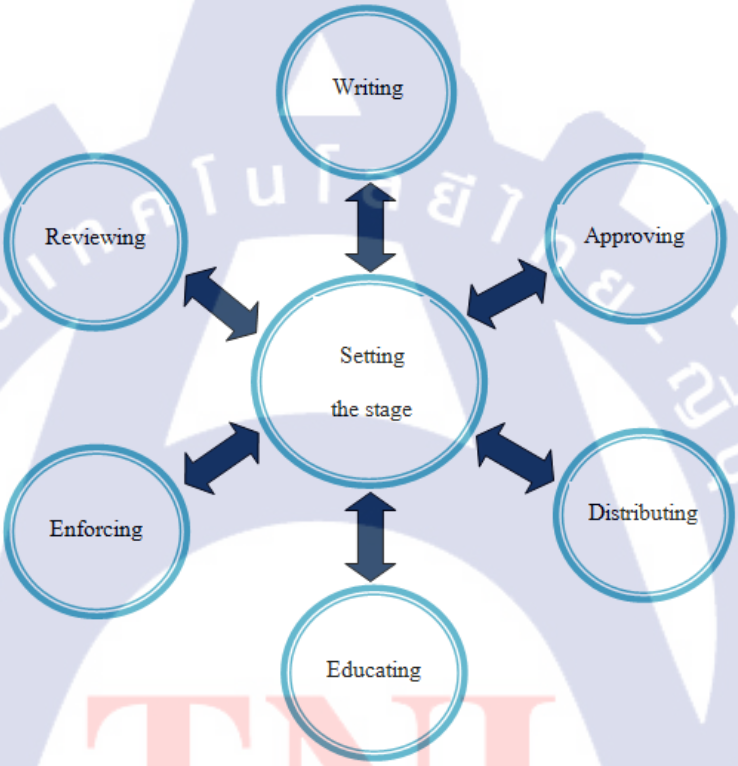
5.1 เอกสารรูปแบบมาตรฐานที่ใช้ในการบันทึกข้อมูล หรือผลลัพธ์ของการปฏิบัติตามข้อกำหนดของนโยบาย ขั้นตอนการปฏิบัติงาน หรือวิธีการปฏิบัติงาน

5.2 เป็นหลักฐานในการปฏิบัติ

ตัวอย่าง

- แบบฟอร์มสัญญาข้อตกลงไม่เปิดเผยข้อมูล
- บันทึกการสำรองข้อมูล
- บันทึกการเข้าปฏิบัติงานในศูนย์คอมพิวเตอร์
- แบบฟอร์มของใช้งานระบบสารสนเทศ

วงจรการพัฒนานโยบายความมั่นคงปลอดภัย



รูปที่ ค.2 วงจรการพัฒนานโยบายความมั่นคงปลอดภัย

1) เตรียมความพร้อมและบริการจัดการ

1.1 ต้องทราบว่าอะไรคือปัญหาที่ต้องได้รับการแก้ไขโดยการพัฒนาและประกาศใช้นโยบาย

- อ้างอิงจากผล Gap Analysis
- อ้างอิงจากผลการประเมินความเสี่ยง หรือแผนการแก้ไขความเสี่ยง
- ประเด็นที่ทราบดีว่าเป็นปัญหาที่ต้องได้รับการแก้ไข

1.2 ระวังอย่าให้มีการพัฒนานโยบายขึ้นมาซ้ำซ้อนกับที่มีอยู่เดิม

1.3 กำหนดทีมงานและผู้รับผิดชอบในการพัฒนานโยบาย

1.4 บางคนเหมาะที่จะเป็นผู้ทบทวนมากกว่าผู้พัฒนา

2) เขียนนโยบาย

2.1 ใช้ภาษาที่อ่านเข้าใจง่าย และกระชับ

- ทุกคนในองค์กรต้องสามารถเข้าใจได้
- ระวังการใช้คำว่า “ควร”
- หากมีการใช้คำย่อ หรือศัพท์เทคนิค ให้จัดทำเป็นอภิธานศัพท์

2.2 พิจารณาจัดทำเอกสารแม่แบบที่ระบุรูปแบบและขนาดของตัวอักษร ตลอดจนการจัดหน้าของเอกสาร

องค์ประกอบของนโยบาย

1) วัตถุประสงค์ คือ ระบุวัตถุประสงค์หรือเป้าหมายของนโยบาย

ตัวอย่าง

“เพื่อกำหนดแนวทางในการรักษาความมั่นคงปลอดภัยให้แก่ทรัพย์สินขององค์กร โดยเฉพาะอย่างยิ่งทรัพย์สินที่เป็นข้อมูลสำคัญในการดำเนินธุรกิจโดยการปกป้องทรัพย์สินเหล่านั้นให้พ้นจากภัยคุกคามและความเสี่ยง ทั้งจากภายในและภายนอกองค์กร ไม่ว่าจะเกิดขึ้นโดยเจตนาหรือไม่ก็ตาม รวมถึงเพื่อลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นจากเหตุละเมิดความมั่นคงปลอดภัย และเพื่อรักษาไว้ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง”

2) ขอบข่าย คือ กำหนดขอบข่ายที่นโยบายครอบคลุมถึง เช่น คน ทรัพย์สิน หรือสถานที่

ตัวอย่าง

“นโยบายนี้ครอบคลุมพนักงานทุกคน ทั้งพนักงานประจำ และพนักงานชั่วคราว รวมถึงบริษัทคู่ค้า บุคคลภายนอก และผู้ให้บริการภายนอกที่เกี่ยวข้องทั้งหมด

3) เนื้อหา คือ เนื้อหาของนโยบาย

ตัวอย่าง

การใช้งานรหัสผ่านอย่างมั่นคงปลอดภัย

- **รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย ห้ามมิให้มีการใช้งาน** User account **ร่วมกันหรือให้ผู้อื่นเข้าใช้งาน** User account **ของตนโดยเด็ดขาด ทั้งนี้ รวมถึงสมาชิกในครอบครัวเมื่อผู้ใช้งานนำงานกลับไปทำที่บ้านด้วย**
- ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่าน User account และรหัสผ่านของตนทั้งหมด
- ผู้ใช้งานทุกคนต้องได้รับการฝึกอบรมเพื่อให้มีความรู้และความตระหนักในการใช้งานรหัสผ่านอย่างถูกต้อง และรับทราบเทคนิคต่าง ๆ ที่ใช้ในการหลอกลวงและนำไปสู่การโจรกรรมข้อมูล

4) เอกสารสนับสนุน

ระบุเอกสารสนับสนุน เช่น นโยบาย ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติงาน หรือแบบฟอร์มที่เกี่ยวข้อง

3) อนุมัตินโยบาย

3.1 ทบทวนร่างนโยบาย

- คณะทำงาน
- ผู้บริหารระดับกลาง
- ที่ปรึกษา
- ผู้บริหารระดับสูง
- ผู้ใช้งาน

3.2 นำเสนอนโยบายให้ผู้อนุมัติ

- ผู้บริหารระดับสูง
- ผู้บริหารระดับกลาง
- บุคคลหรือคณะทำงานที่ได้รับมอบหมาย

4) แจกจ่ายนโยบาย

4.1 สร้างช่องทางในการสื่อสารนโยบายใหม่ หรือที่ได้รับการปรับปรุง

- อีเมล
- อินทราเน็ต

4.2 ข้อกำหนดด้านความมั่นคงปลอดภัย

- ใช้ภายในองค์กรเท่านั้น
- อ่านอย่างเดียว
- ไม่สามารถทำสำเนาหรือพิมพ์ได้ (ยกเว้นแบบฟอร์ม) **

4.3 ระบุชื่อผู้ติดต่อเพื่อสอบถามข้อมูลเพิ่มเติม

5) สื่อสาร/ให้ความรู้เกี่ยวกับนโยบาย

5.1 พนักงานใหม่

5.1.1 แจ้งให้พนักงานใหม่ทราบในวันปฐมนิเทศ:

- จัดฝึกอบรม
- แจกจ่ายเอกสาร
- วีดีโอประชาสัมพันธ์
- ให้พนักงานใหม่ลงนามยอมรับการปฏิบัติตามนโยบาย

5.1.2 ใช้ระบบสารสนเทศเข้าช่วย

- Log-on banner

5.1.3 อีเมล์แจ้ง

5.2 พนักงานปัจจุบัน

5.2.1 สื่อประชาสัมพันธ์ต่าง ๆ เช่น โปสเตอร์

5.2.2 จัดฝึกอบรม

- สัมมนาใหญ่
- อบรมกลุ่มย่อย
- Web-based/E-Learning
- On-the-job

6) บังคับใช้นโยบาย

6.1 ประเด็นเรื่องการบังคับใช้นโยบาย

6.1.1 หากไม่สามารถบังคับใช้นโยบายได้จริง

- ไม่สามารถลดความเสี่ยงขององค์กรได้
- ไม่ผ่านการตรวจรับรองตามมาตรฐาน ISO 27001

6.1.2 องค์กรต้องมีพนักงานเพียงพอที่จะควบคุมและติดตามบังคับใช้นโยบาย

6.1.3 จัดตั้งส่วนงานย่อย หรืออย่างน้อยกำหนดให้มีบุคคลที่ทำหน้าที่ในการควบคุมและติดตามการบังคับใช้นโยบาย

7) ทบทวนและปรับปรุงนโยบายตามรอบระยะเวลาที่เหมาะสม

7.1 ทบทวนและปรับปรุงนโยบายอย่างสม่ำเสมอ

7.1.1 กำหนดผู้รับผิดชอบนโยบายแต่ละฉบับ หรืออย่างน้อยกำหนดให้มีบุคคลที่ทำหน้าที่ในการดูแลนโยบายทั้งหมด

7.1.2 กำหนดรอบระยะเวลาในการทบทวน

7.1.3 จูงใจให้มีการเสนอแนะเพื่อปรับปรุงนโยบาย

7.1.4 จัดเก็บนโยบายเวอร์ชั่นเก่า และบันทึกประวัติการปรับปรุงเอกสาร

7.1.5 วัดผลสำเร็จด้วยการเฝ้าติดตาม และการตรวจสอบ

การดำเนินการให้การจัดทำนโยบายและแผนงานประสบความสำเร็จในการนำไปใช้จริง

แนวทาง

1) กำหนดวาระการประชุม เพื่อติดตามผลการดำเนินงาน
2) ผู้บริหารสูงสุดขององค์กรต้องคอยติดตามและกระตุ้น
3) รายงานความคืบหน้าในการดำเนินงานตามนโยบายอย่างสม่ำเสมอ
4) จัดประชุมเพื่อทบทวนการดำเนินงานตามนโยบายและแผนงานของแต่ละฝ่ายเป็นการล่วงหน้า
5) ทำการประชาสัมพันธ์และกระตุ้น เตือนให้สมาชิกในองค์กรเข้าร่วมกิจกรรมที่จัดขึ้นตามนโยบายและแผนงานอย่างต่อเนื่องและสม่ำเสมอ

การพัฒนานโยบายความมั่นคงปลอดภัยให้มีประสิทธิผล

นโยบายที่ดีต้องมีคุณสมบัติ ดังนี้

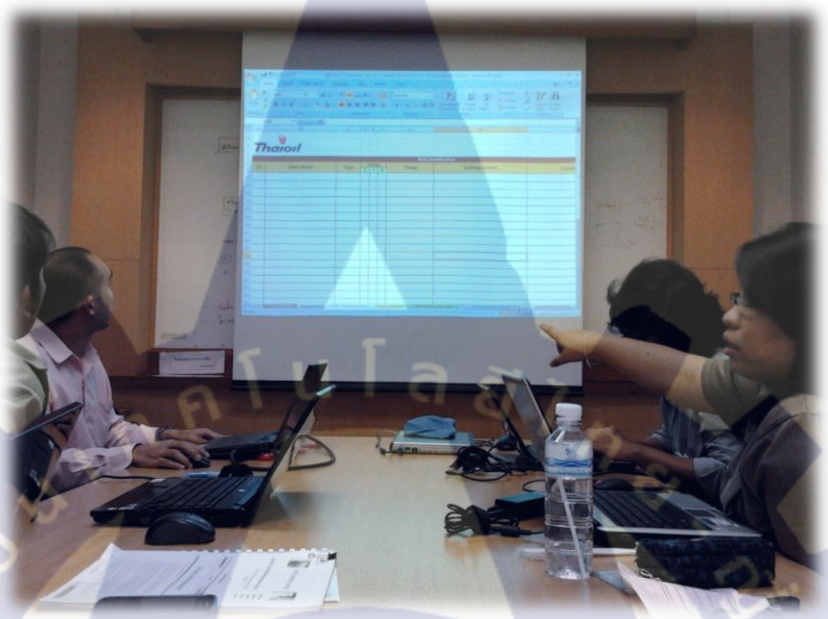
1) ตรงจุด (Specific)
   - สามารถแก้ปัญหาขององค์กรได้
2) วัดผลได้ (Measurable)
   - วัดผลสำเร็จที่เป็นรูปธรรมได้
3) ปฏิบัติได้ (Achievable)
   - จัดทำเอกสารสนับสนุน และให้เครื่องมือแก่พนักงานในการปฏิบัติตามนโยบาย

4) สมเหตุสมผล
   - สามารถปฏิบัติได้จริง
   - ให้เวลาในการบังคับใช้นโยบาย
5) เวลาเหมาะสม (Time based)
   - ระบุเวลาที่บังคับใช้
   - ระบุเวลาที่จะทำการทบทวนและปรับปรุง
   - ระบุเวลาที่จะทำการตรวจสอบ

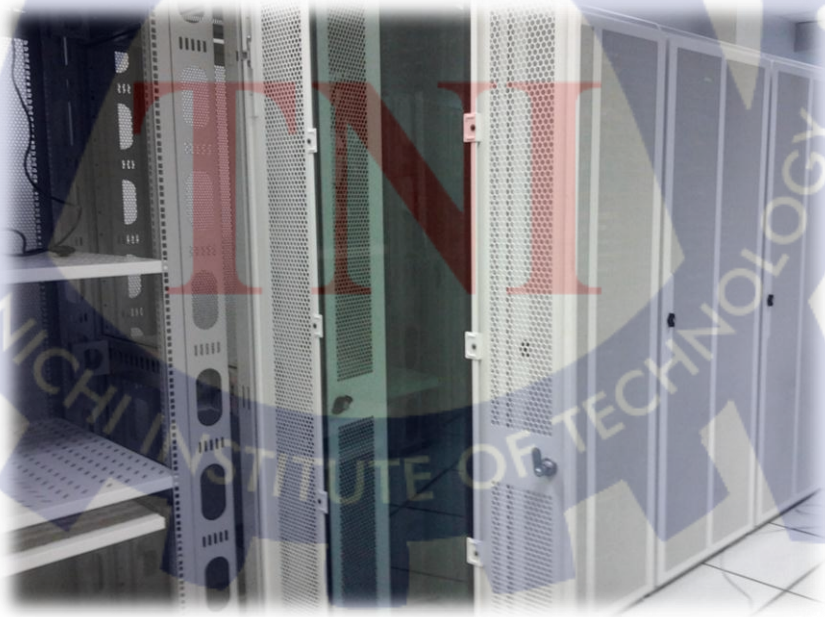
สรุป

1) การเขียนนโยบายนั้นไม่ยาก การบังคับใช้คือสิ่งที่ยาก
2) ผู้บริหารมีส่วนสำคัญอย่างยิ่งในการพัฒนาและบังคับใช้นโยบายให้มีประสิทธิผลและลดความเสี่ยงขององค์กร
3) ให้ทุกคนมีส่วนร่วมในการพัฒนาและทบทวนนโยบาย เพื่อลดปัญหาในการต่อต้านหรือการละเมิดนโยบาย
4) นโยบายต้องสอดคล้องกับวัฒนธรรมองค์กร

ภาคผนวก ง
รูปถ่ายผลงานสหกิจศึกษาที่ได้ดำเนินการในห้องศูนย์คอมพิวเตอร์



รูปที่ ง.1 ประชุมทำ Risk Treatment Plan



รูปที่ ง.2 จัดวางตู้เพื่อใส่ Server สำรอง

รูปที่ ง.3 ติดตั้ง Server สำรอง

รูปที่ ง.4 การติดตั้งระบบปฏิบัติการ Window Server ในเครื่อง Server สำรอง

รูปที่ ง.5 การจัดซื้อ Server

รูปที่ ง.6 จัดเก็บเทปบันทึกข้อมูลใส่ตู้ล็อค

รูปที่ ง.7 วิธีการเก็บข้อมูลสำรองระหว่างส่งไปให้บริษัทจัดเก็บสื่อบันทึก

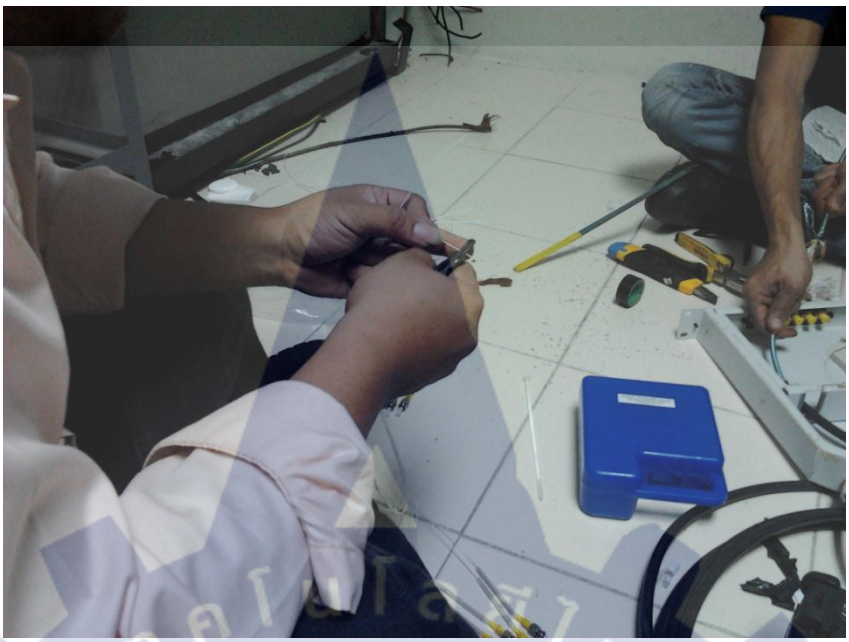
ภาคผนวก จ

รูปถ่ายผลงานสหกิจศึกษา เรื่อง การเดินสาย Cable และติดตั้ง Wireless

1. ติดตั้งเดินสายเคเบิ้ล

รูปที่ จ.1 เริ่มเดินสาย Cable เข้าตึกใหม่

รูปที่ จ.2 ใส่ปลอกหนาเพื่อกันสาย Cable แตก

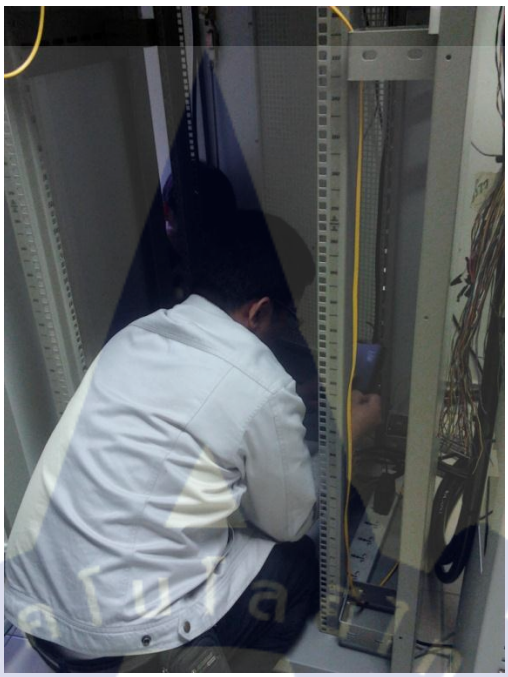


รูปที่ จ.3 ปลอกสาย Cable

รูปที่ จ.4 นำสายเคเบิ้ลใส่กล่องเพื่อใช้ในการเชื่อมต่อ

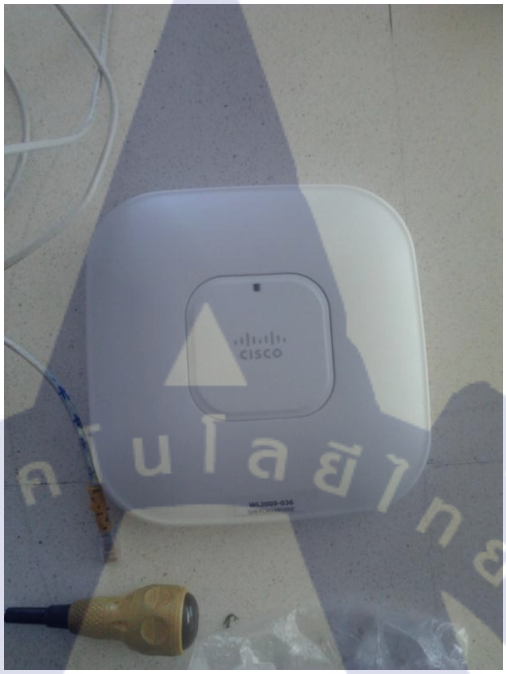
รูปที่ จ.5 ภายในกล่องเชื่อมสาย Cable และพร้อมใช้ในการเชื่อมต่อ

รูปที่ จ.6 ติดตั้งตัวส่งสัญญาณ

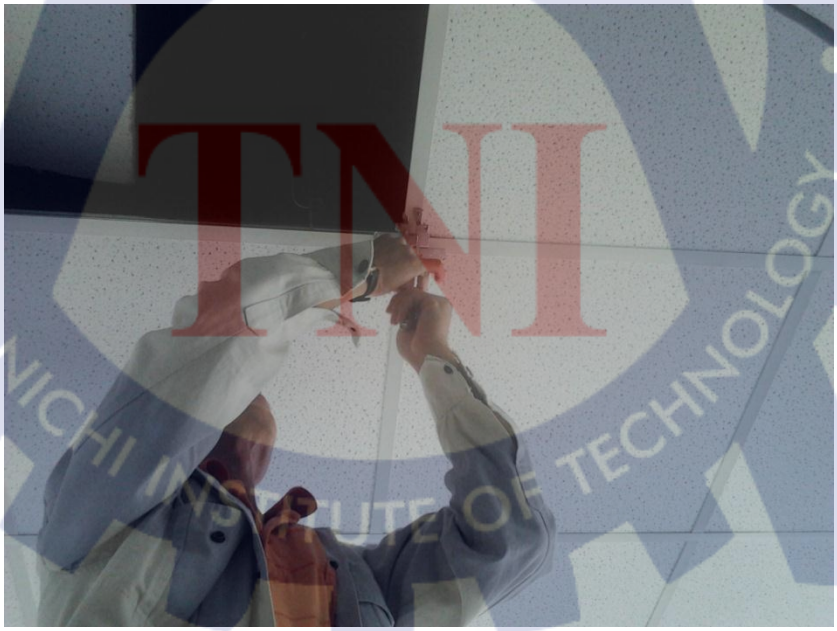


รูปที่ จ.7 ติดตั้งตัวส่งสัญญาณ

2. ติดตั้ง Wireless

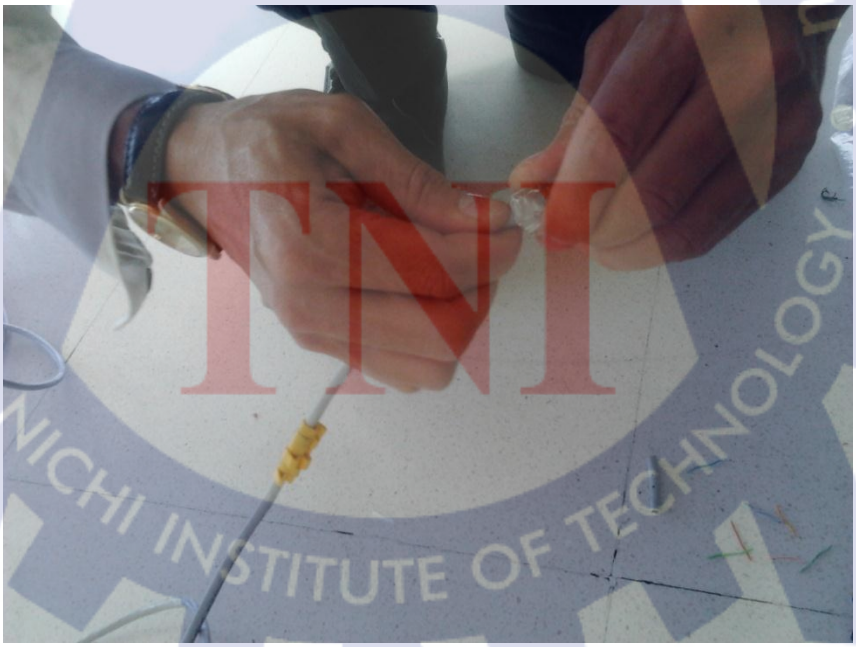


รูปที่ จ.8 เครื่องกระจายสัญญาณ Wireless



รูปที่ จ.9 ติดตั้งเครื่องกระจายสัญญาณ Wireless

รูปที่ จ.10 ติดตั้งเครื่องกระจายสัญญาณ Wireless



รูปที่ จ.11 ติดตั้งเครื่องกระจายสัญญาณ Wireless

รูปที่ จ.12ติดตั้งเครื่องกระจายสัญญาณ Wireless

รูปที่ จ.13 ติดตั้งเครื่องกระจายสัญญาณ Wireless

รูปที่ จ.14 ส่งสัญญาณให้กับตัวกระจายสัญญาณ

รูปที่ จ.15 ส่งสัญญาณให้กับตัวกระจายสัญญาณ

ภาคผนวก ฉ
ประมวลคำย่อ

CEO	Chief Executives Officer (ประธานบริหาร)
AMD-C	Assistant Managing Director – Corporate Affairs (ผู้ช่วยกรรมการผู้จัดการฝ่ายองค์กรสัมพันธ์)
DMD-R	Deputy Managing Director – Refinery (รองกรรมการผู้จัดการฝ่ายโรงกลั่น)
HR	Human Resource Manager (ผู้จัดการฝ่ายทรัพยากรมนุษย์)
DMD-B	Deputy Managing Director – Business (รองกรรมการผู้จัดการฝ่ายธุรกิจ)
CP	Corporate Commercial Planning Manager (ผู้จัดการฝ่ายวางแผนพาณิชย์)
CM	Commercial Manager (ผู้จัดการฝ่ายพาณิชย์)
PD	Asset Development Manager (ผู้จัดการฝ่ายพัฒนาสินทรัพย์)
AMD-R	Assistant Managing Director – Refinery (ผู้ช่วยกรรมการผู้จัดการฝ่ายโรงกลั่น)
SP	Strategic Planning Manager (ผู้จัดการฝ่ายวางแผนกลยุทธ์)
MF	Operation Manager (ผู้จัดการฝ่ายปฏิบัติการ)
MQ	Product & Quality Manager (ผู้จัดการฝ่ายผลิตภัณฑ์และคุณภาพ)
EN	Engineering Manager (ผู้จัดการฝ่ายวิศวกรรม)
TN	Technology Manager Zผู้จัดการฝ่ายเทคโนโลยี)
SPIS	Strategic Planning of Information Systems Department (แผนกกลยุทธ์ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร)
PTTICT	Petroleum Authority of Thailand's Information and Communication Technology Department (แผนกเทคโนโลยีสารสนเทศและการสื่อสารบริษัทการปิโตรเลียมแห่งประเทศไทย)

ประวัติผู้วิจัย

ชื่อ - นามสกุล นางสาววรรณภา มงคลกิจจาวงศ์

วัน เดือน ปีเกิด 9 พฤศจิกายน 2532

ประวัติการศึกษา

ระดับประถมศึกษา ประถมศึกษาตอนปลาย พ.ศ. 2544
โรงเรียนเรวดี

ระดับมัธยมศึกษา มัธยมศึกษาตอนปลาย พ.ศ. 2550
โรงเรียนสามเสนวิทยาลัย

ระดับอุดมศึกษา คณะวิศวกรรมศาสตร์ สาขาวิศวกรรมคอมพิวเตอร์ พ.ศ. 2551
สถาบันเทคโนโลยีไทย - ญี่ปุ่น

ทุนการศึกษา -ไม่มี-

ประวัติการฝึกอบรม ISO 27001-ISO27002 ISMS Implementation Training
ที่ Thai Oil Public Company Limited

ผลงานที่ได้รับการตีพิมพ์ -ไม่มี-